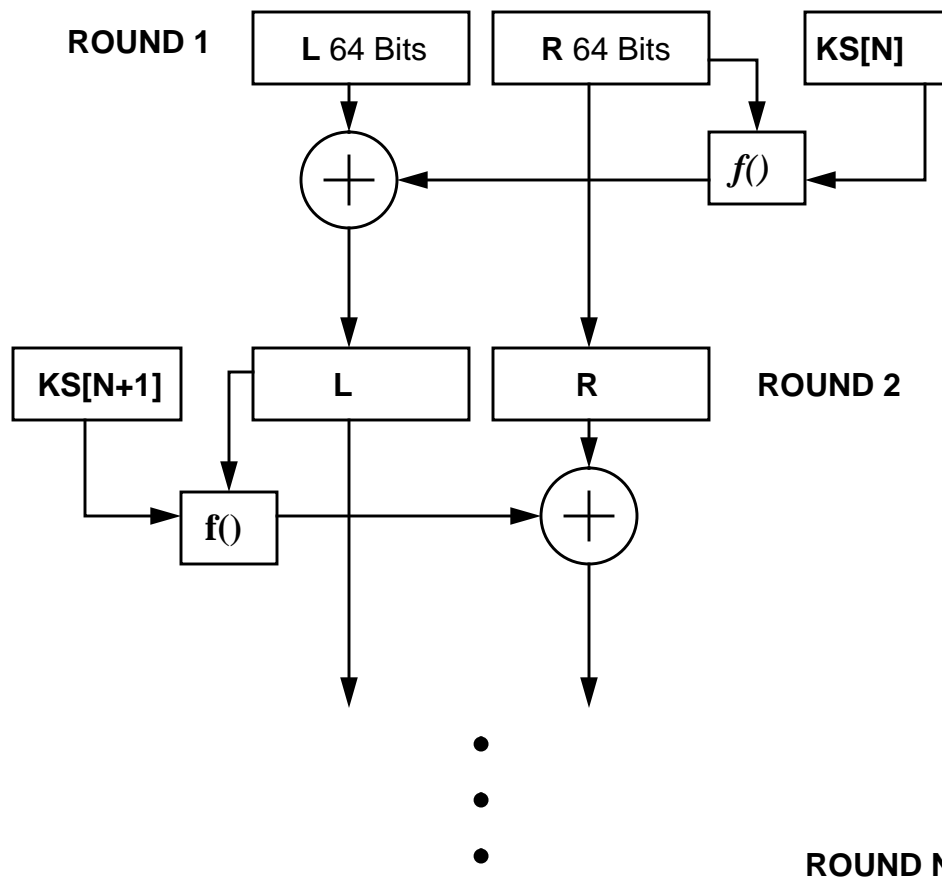


CRISP: A Feistel cipher with hardened key-scheduling

Marcus Leech, Nortel Technologies

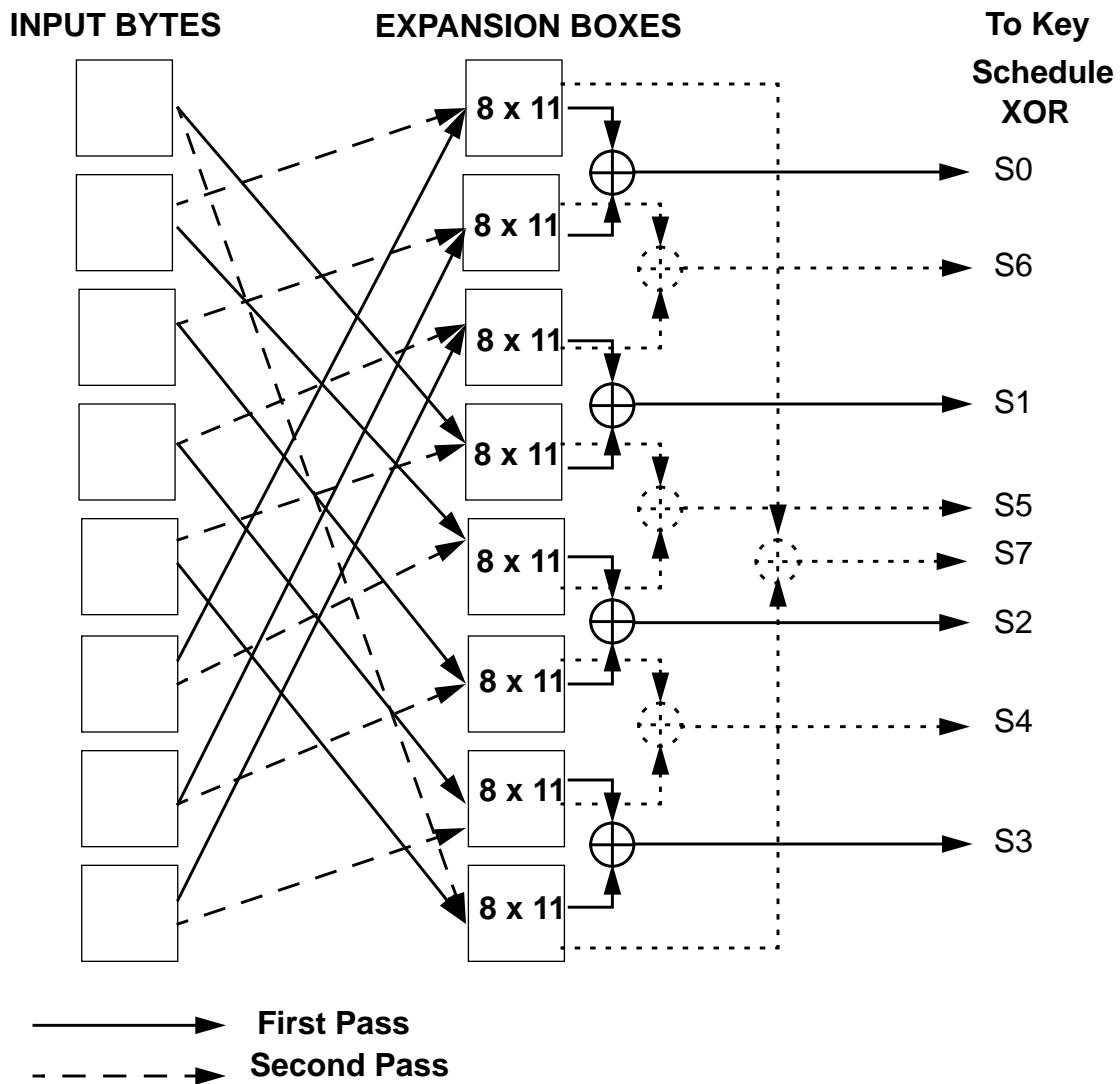
Algorithm

This paper describes a new Feistel block cipher, *CRISP*, that uses itself as a PRNG in the key-scheduling function. The cipher consists of 6 rounds in which the left and right half input blocks are alternately modulo-2 added to a non-linear function of the other half input block, and the current key schedule bits.



The cipher uses a 128-bit key, with a 128-bit data block. The non-linear round function, $f()$, computes a permute-substitute function of the current 88-bit key-schedule bits with the 64 input bits. The 64-bit input is first expanded to 88-bits using XOR-combined 8x11 bit S-boxes. The result of the expansion is then XORed with the 88 key bits, and fed through eight 11x8 S-boxes. The output of the S-boxes is then processed through $S2()$, a function that uses five 8x32 S-boxes that are

The $ES()$ expansion function is defined as follows:



Example values for the $ES()$ function tables are listed in Appendix A.

S-Box design methodology

The primary S-boxes in *CRISP* are constructed according to design principals described in an article on S-box design by Gordon and Retkin[1]. In that article, they make the claim that the probability of linearity of an S-box is proportional to the inverse of the factorial of its size. Each S-box is based on a composition of eight 8x8 reversible, randomly permuted S-boxes. That is, for an 11-bit input, the low-order 8 bits select an 8-bit value from an 8x8 S-box, while the high-order 3 bits select which 8x8 S-box to use. This is identical to the structure used in the DES S-boxes.

The primary S-boxes are generated using a C program designed to find S-boxes with a given threshold pairs-XOR count and threshold linearity; the program generates random S-boxes, measures the maximum pairs-XOR count, and linearity and discards any S-boxes whose pairs-XOR count is above the threshold, or whose linearity is above the threshold. Linearity is computed by

measuring the hamming distance between all possible output vectors (combined under XOR) against all linear-boolean function vectors of the input bits. The resulting minimum hamming distance is then compared to the threshold; S-boxes with a lower minimum hamming distance are rejected.

If the resulting S-box passes both the differential and linearity tests, it is also tested against the first-order *Bit Independence Criterion* test, to ensure that no pairs of S-box output bits change together more than 50% of the time, when the input changes by a single bit.

The evaluated version of *CRISP* uses S-boxes with a pairs-XOR threshold value of 30, and minimum hamming distance of 0.45215 (926 / 2048). The value 30 for the pairs-XOR threshold was chosen because of a currently-uninvestigated runtime complexity phenomenon. When generating random S-boxes in this way, the execution time of the generator increases non-linearly as the threshold value decreases. It was determined that below a threshold value of 30, the program tended towards infinite execution time. Initially, it was thought to be an artifact of the random-number generator in use, so a new one was inserted, with exactly the same result. In any case, the goal of the generator program is to reduce the maximum pairs-XOR count towards the perfect value, which in the case of 11x8 S-boxes is 8 ($2^{11} / 2^8$). The value 30 corresponds to a single-round, single S-box probability of 1.46×10^{-2} .

The $S()$ generation process requires approximately 40 CPU-hours on an HP9000/735.

Examples of S-boxes that correspond to the selection criteria are listed in Appendix B.

S2() function design

The $S2()$ consists of five 8x32 S-boxes, generated in a key-dependant way. These 8x32 S-boxes are used twice on the 8-bit outputs of the primary S-boxes to produce a 64-bit final result.

The $S2()$ function provides an extra stage of confusion and diffusion within the round function. It has the important added benefit of adding to the overall complexity of differential cryptanalysis, reducing the single round, single S-box probability from 1.46×10^{-2} to 8.82×10^{-7} ($0.0146 * (0.0078)^2$). This comes from recent results[2] on the differential cryptanalysis properties of random 8x32 S-boxes.

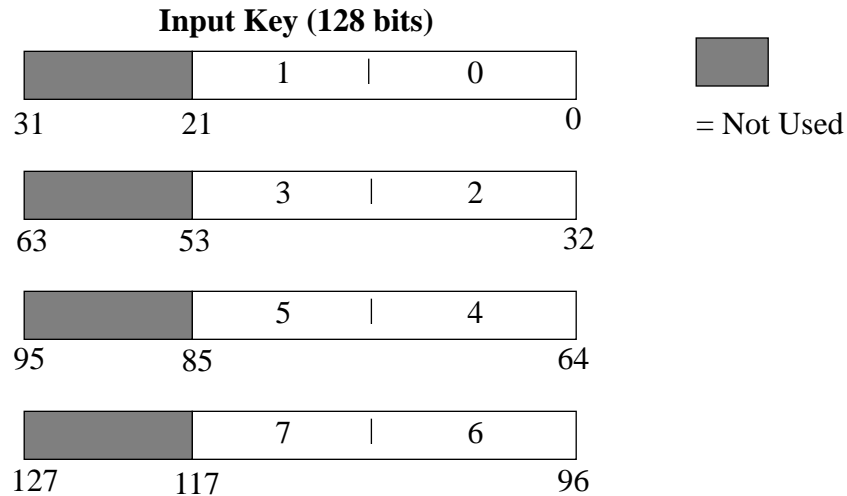
Since the contents of the $S2()$ S-boxes are unknown to the cryptanalyst, both linear and differential cryptanalysis are significantly hampered.

Subkey generation

Subkeys are generated in such a way that if a given subkey is determined by cryptanalysis, it is cryptographically difficult to determine the other subkeys from the known subkey.

This is achieved by using the basic *CRISP* encryption function as a pseudo-random number generator, using the key as a seed. This is accomplished in a multi-step process, described below.

First, a “standard” key-schedule is loaded into the *CRISP* function, the standard key-schedule is derived from the first 48 entries in table 0 and table 7 in the *ES()* function, combined with XOR. This standard key-schedule is then perturbed by selecting bits from the input key, and XOR combining them with the “standard” key schedule, 11 bits at a time. A total of 88 bits from the input key are selected for use in perturbing the “standard” key schedule, as follows:



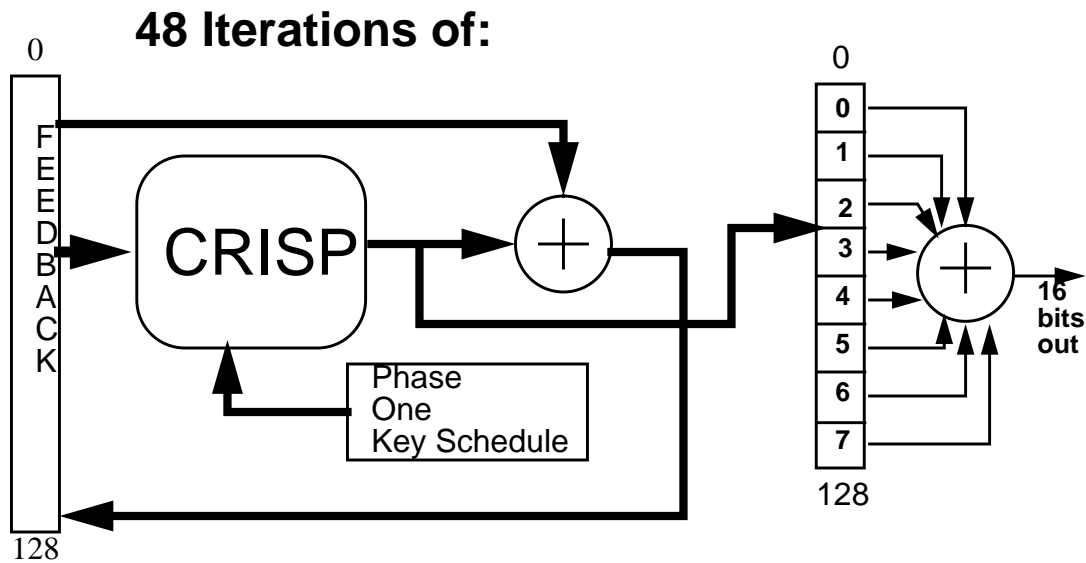
The 48 entries from the *ES*[0,7] XOR are grouped into six sets of eight elements, producing the following table.

Table 1: Standard Key Schedule

Round	0	1	2	3	4	5	6	7
1	4CC	079	4AA	7BC	6C8	573	3DE	5EC
2	63F	6EF	2BF	1AE	7F2	253	595	42E
3	5E3	24B	7CB	1D9	324	341	2E6	1E2
4	142	47C	26D	593	151	028	23D	004
5	527	39F	30C	217	01D	7A6	55B	1DB
6	7FA	271	64E	4B4	316	53A	2B8	3A9

Each row in this table is XORed with the corresponding (0 through 7) 11-bit value extracted from the key. This slightly-perturbed key-schedule (*phase one* key-schedule) is then used in a feedback execution of *CRISP*, to produce a new key-schedule. The feedback begins by using the key as the initial cleartext, on each iteration, the feedback buffer is updated by XOR with the *CRISP* ciphertext output. This *phase two* key-schedule is produced by using each output of the feedback execution of *CRISP* to produce 11-bit key-schedule elements that update the *phase one* schedule by one

element on each iteration, for a total of 48 iterations. The diagram below illustrates this concept:



The final key schedule is produced by again using *CRISP* in a feedback mode, with the input key as the initial cleartext, using the *phase two* key schedule, and the standard *S2()* function. Each ciphertext output is considered as eight 16-bit values, each of which is XORed together, then masked down to 11 bits to produce a key-schedule element. This process is repeated until all of the key-schedule elements have been filled. There are eight 11-bit elements per round, with six rounds in the evaluated implementation, for a total of 48 key schedule elements or 528 key schedule bits.

Generation of the *S2()* function

The *S2()* function is computed in a similar fashion to the final key-schedule, using *CRISP* in feedback mode. This feedback execution is a continuation of the feedback execution used in generating the final key-schedule. Each output of the *CRISP* execution is considered as four 32-bit values. The values are combined using XOR, with the resulting value being placed in the next available *S2()* table element. If the 32-bit value has already been used in an *S2()* table element, it is discarded and a new value is generated.

There are five *S2()* tables, each with 256 entries, for a total of 1280 32-bit elements.

Comparison of *CRISP* and *DES* round functions

The round function of DES takes a 32-bit input, and computes a non-linear function of that 32-bit input. It accomplishes this using four discrete steps. The 32-bit data input is expanded using the E expansion, then mixed with the 48-bit key-schedule bits. The resulting 48-bit value is then non-linearly substituted using the eight 6x4 S-boxes. The final step is to permute the 32-bit S-box output using the P permutation.

When examining the *E* expansion in DES, notice that it provides no guarantee that a given input bit can affect more than one S-box. This makes differential cryptanalysis easier, since single S-

boxes can be “isolated” for differential cryptanalysis purposes.

The cryptographic significance of the P permutation is assumed to be for the purposes of improving the diffusion properties of the round function, since the E expansion provides rather less diffusion.

The *CRISP* algorithm has the same basic structure in its round function as DES. The round function takes a 64-bit input, expands it to 88 bits using the ES function, mixes it with the key, and non-linearly substitutes the 88-bits using eight 11x8 S-boxes. When examining the ES function, observe that each input bit affects two S-boxes, thus making differential cryptanalysis somewhat harder. The ES function also provides, as a secondary effect, a small amount of non-linearity, since it acts as a 16x11 S-box. The *CRISP* S-boxes, due to their size, provide higher a degree of resistance both to differential and linear cryptanalysis than DES.

In *CRISP*, the post S-box function, $S2$, corresponds roughly to the P permutation in DES. Observe that $S2$ provides a non-linear transform of the S-box outputs, while the P function in DES is entirely linear. The $S2$ function also improves resistance to both differential and linear cryptanalysis, since the $S2$ table elements are unknown to the cryptanalyst. Even if the cryptanalyst is able to determine the contents of $S2$, it is assumed that the analysis of random 8x32 S-boxes, as described in [2], would hold for the $S2$ function within *CRISP*.

Analysis of key-scheduling and $S2()$ generation

The strength of the key-scheduling and $S2()$ function generation algorithm is predicated on the ability of the concatenation of round functions to act as a random, non-linear transform of the input key material. The avalanche results shown later tend to suggest that *CRISP* does act as a strong random transform, with good per-round non-linearity; the assumption is that the concatenation of rounds produces a non-linearity that is close to the product of the non-linearity of the round function.

The purpose of the key-schedule algorithm is to produce a sequence of bits from the input key material that can be used as per-round keys. Many encryption functions use a key-schedule algorithm in which the round key bits are related to the input key in a way that is linear. The DES, for example, uses a series of rotates and selects to produce round key material. This makes DES slightly more vulnerable to differential cryptanalysis[4] than DES with purely-random, independent round keys. This occurs because determination of one or more per-round key bits results in determination of related bits in other rounds.

It has been proposed, most recently in [5], that the DES can be strengthened somewhat against both linear and differential cryptanalysis by using the DES cipher itself as a PRNG in the generation of key-schedule bits.

The Blowfish[7] cipher also uses itself as a PRNG in the generation of both its S-boxes, and in the generation of the $P()$ round function.

An early version of *CRISP* used MD5[6] as a PRNG in the generation of round keys, but it was

felt to be overly complex, and not as compact as a key-scheduling algorithm that uses the *CRISP* cipher itself as a PRNG.

If we assume that the cryptanalyst is able to determine the round key at a particular round, they must be able to determine the plaintexts that correspond to the partial ciphertexts that constitute the determined round key. Each 11-bit round-key element is the XOR of eight 11-bit sections of a *CRISP* ciphertext, under an unknown key, with unknown plaintext. The problem, then, is to determine the full 128-bit ciphertext, and the corresponding plaintext, under an unknown key.

The cryptanalyst has a similar problem to solve when they are able to determine some values within $S2()$. They must first determine, for a given determined 32-bit S-box entry value, the corresponding 128-bit ciphertext, then the key-schedule and plaintext that produced it.

The performance of key-scheduling is entirely dependant on the performance of the *CRISP* algorithm itself. The *CRISP* algorithm is called approximately¹ 1376 times in setting a new key. On the hardware the algorithm was tested on, this corresponds to 20 milliseconds of real time. This could be improved by changing the algorithm that produces $S2()$ to produce four $S2()$ elements at a time from the full-width 128-bit output of *CRISP*.

Avalanche Results

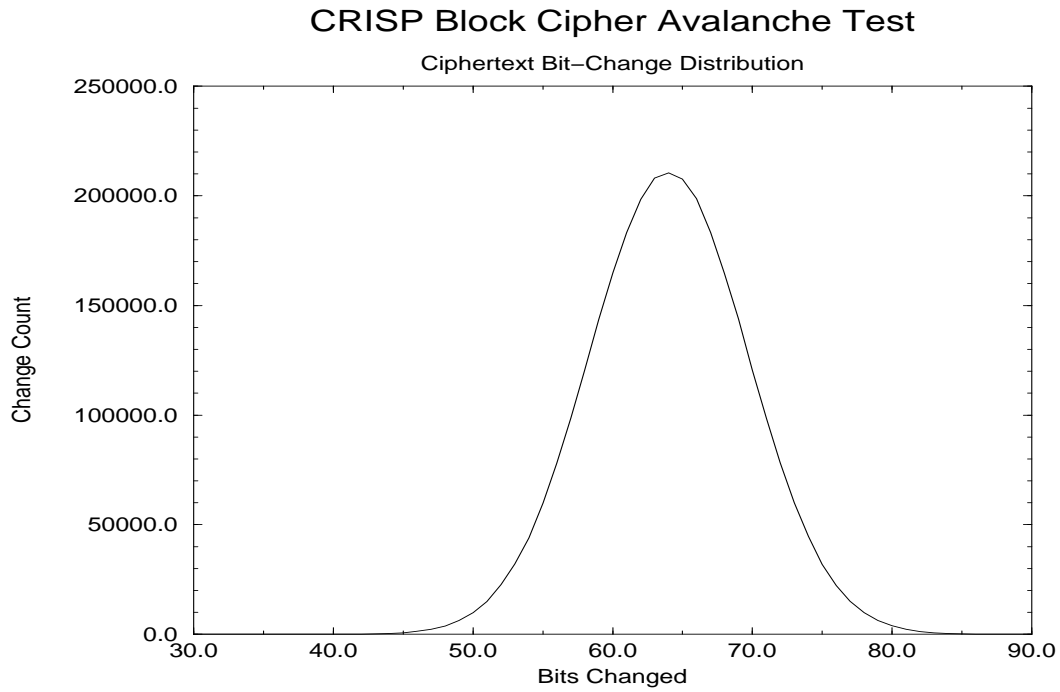
The avalanche properties were measured by iterating the *CRISP* encryption function 3,000,000 times, using a fixed, random key, and a random data input that is modified randomly by one bit on each iteration. This process was repeated several times.

This results in an average change in the resulting ciphertext of 64 bits, which is 50% of the total ciphertext bits. The minimum change ranges from 35 to 37, while the maximum ranges from 85 to 92. The minimum ciphertext change corresponds to somewhat more (0.273 to 0.289) than 25% of the total bits in the ciphertext.

The DES under similar test conditions tends to produce an average ciphertext change of exactly 50% of the bits, while the minimum is usually somewhat less (0.203 to 0.234). The following

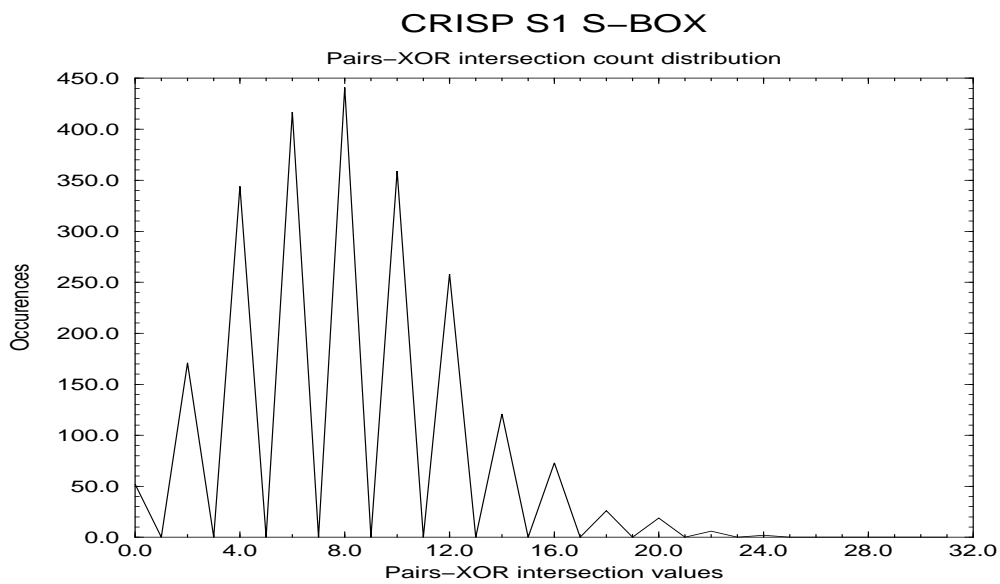
1. Since the $S2()$ generation process can potentially call *CRISP* a variable number of times, due to its selection criterion.

graph shows the distribution of ciphertext bit-changes for 3,000,000 iterations of the function:



Differential Cryptanalysis Results

The pairs-XOR count distribution graph shows that the mean value for a pairs-XOR “intersection” over the entire S1 box from $S()$ is 8:



This graph requires some explanation. The usual method to show pairs-XOR distribution uses a table, with the output-XOR as columns, and the input-XOR as rows. The elements of such a table convey the distribution of pairs-XOR values over the given S-box. The *CRISP* S-boxes are 11x8, which means the resulting table would have 256 columns and 2048 rows; values that yield a rather ungainly tabular display. The graph conveys the same overall information, showing that the “intersection” values are clustered around the so-called perfect distribution that would be achieved if each intersection in the pairs-XOR table were equally likely. In the *CRISP* case, that perfect distribution value would be 8 ($2^{11} / 2^8$).

We can observe from the pairs-XOR distribution, that all of the primary S-boxes have the same maximum pairs-XOR value of 30 (or a probability of 0.0146). There is no obvious advantage to attacking a particular S-box over another.

The $ES()$ function effectively acts as a fixed 16-to-11 bit mapping between bits of the round function input, and input bits to a single S-box. The following table illustrates the mapping:

Table 2: ES function input mapping

Input Octet Pair	ES box pair	S-box affected
5 and 6	0 and 1	S0
7 and 0	2 and 3	S1
1 and 2	4 and 5	S2
3 and 4	6 and 7	S3
7 and 6	6 and 5	S4
5 and 4	4 and 3	S5
3 and 2	2 and 1	S6
1 and 0	0 and 7	S7

In effect, a new set of 16-by-11 bit S-boxes are synthesized by the input mapping to $ES()$.

The problem for the cryptanalyst, then, is to find input octet pairs that produce the maximum differential probability (by minimizing the number of S-boxes involved, and by selecting the highest probability for each S-box involved). In DES, the pre-S-box expansion function, E , has the property that for input pair X_1 and X_2 the equation $E(X_1) XOR E(X_2) = E(X_1 XOR X_2)$ is always true. In *CRISP*, the equivalent $ES(X_1) XOR ES(X_2) = ES(X_1 XOR X_2)$ is true for only a small number of input pairs (approximately 1 in 2500). This means that a different approach is required when engaging in differential cryptanalysis. The cryptanalyst must search for input pairs that satisfy the equation $ES(X_1) XOR ES(X_2) = I$, where I is a desirable input XOR to a target S-box. Because each such input pair controls both the so-called *target* S-box, and partially controls the input to

two other S-boxes, via different $ES()$ boxes, it is thought to be difficult to find input pairs that simultaneously satisfy desirable input XOR conditions for the S-boxes they control.

Initial analysis of the density of pairs satisfying the criterion of a high-probability XOR in one S-box, while having a zero XOR in the two other S-boxes linked via common input octets is estimated to be 1 in 2^{28} , for randomly selected inputs. For example, S-box 0 is linked to S-box 4 and S-box 5 via input octets 5 and 6. This means that the input to these three S-boxes is fully defined by 4 input octets, (octets 4,5,6 and 7). The following input pairs for octets 4,5,6,7 satisfy the above criterion:

```

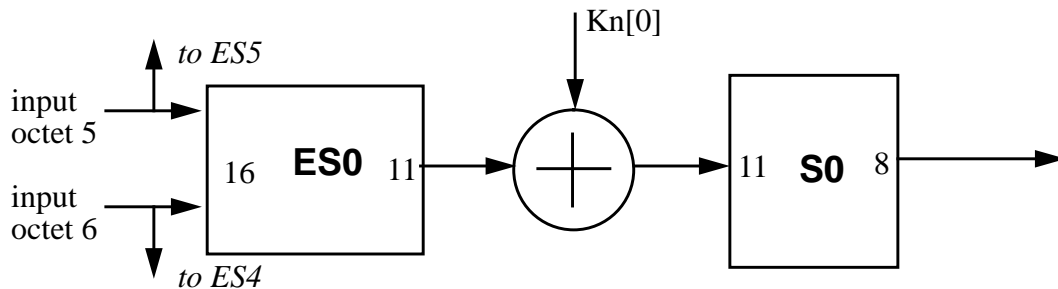
X1=7068790E X2=D68D3980
X1=09FC3D28 X2=2898D918
X1=493238F2 X2=CBF8D398
X1=40D72FF9 X2=5465FB57

```

The above input values do not necessarily guarantee zero input XOR to the other S-boxes affected by input octets 4 and 7 (S-boxes 3 and 1).

It is surmised that inputs satisfying the more stringent criterion of having a high-probability input XOR in one S-box, while having zero XOR in all the others have a very low density. Similarly, inputs satisfying the criterion of having high-probability in two S-boxes, while having zero XOR in all other S-boxes is of a similar density. Initial testing shows that the density may be less than 1 pair in 2^{34} random input pairs.

The combined $ES()$ and $S()$ can be re-arranged (with S_0 as example), as follows:



Given the above arrangement, we can compute the input XOR distribution for $ES()$ that yields the high-probability input XORs to the corresponding $S()$ S-box. The S_0 box, for example, has 12 high-probability inputs XORs (that is input XORs, that have output XORs occurring with probability 0.0146). In S_0 , a high-probability input XOR is $X'6AE'$. An input XOR of $X'03AA'$ to ES_0 leads to an ES_0 output XOR of $X'6AE'$ which in turn leads to an output XOR in S_0 of $X'17'$, with compound probability 1.79×10^{-5} . The following table shows examples of the highest com-

pound probabilities of ES0 input XORs producing a given S0 output XOR.

Table 3: Example ES0/S0 XOR probabilities

ES[0] Input XOR	S[0] Output XOR	Probability
X'054F'	X'E9'	2.15E-5
X'0DAD'	X'B8'	2.06E-5
X'6635'	X'97'	2.06E-5
X'700E'	X'17'	2.24E-5
X'7B13'	X'97'	2.15E-5
X'81CB'	X'DA'	2.06E-5
X'8233'	X'4D'	2.06E-5
X'FD28'	X'97'	2.06E-5

Since each input octet controls two S-boxes, a reasonable assumption to make is that at least two S-boxes must be “involved” in a given single-round characteristic, thus giving a maximum single-round probability near 4.8×10^{-10} (X'700E' to X'17'). If we assume that a six-round characteristic can be constructed in which half the rounds have probability 1, and half the rounds have the probability 4.8×10^{-10} , then without S2(), *CRISP* is theoretically vulnerable to differential cryptanalysis, since the resulting probability near 1.10×10^{-28} is greater than the probability near 2.9×10^{-40} that would be necessary to make *CRISP* unconditionally resistant to differential cryptanalysis. If, however, the best characteristic that can be constructed uses the probability of 4.8×10^{-10} in all but one round, with a probability 1 characteristic in one round, then *CRISP* would be unconditionally resistant to differential cryptanalysis, since the resulting probability is near 2.5×10^{-47} . No attempt has yet been made so find the best 6-round characteristic for *CRISP*, since S2() is assumed to defeat differential cryptanalysis.

If an *average-case* S2() function is factored into the differential probability analysis, then the algorithm is unconditionally resistant if the best six-round characteristic has probability 1 in three of the rounds, and probability near 2.92×10^{-14} in the other rounds, producing an aggregate probability near 2.55×10^{-41} .

Appendix C contains complete tables of high-probability XORs for the eight ES/S combinations.

Linear Cryptanalysis Results

Work on linear cryptanalysis is in progress at the time of writing.

Resistance to the Birthday Paradox under CBC

Under Cipher Block Chaining mode, this cipher is more resistant than ciphers with smaller block

sizes to the Birthday Paradox, which states that, if $2^{n/2}$ plaintexts are encrypted under CBC (where n is the blocksize in bits), the probability of there being two equal ciphertexts is 0.5. If two identical ciphertexts correspond to different plaintexts, then there exists a known XOR relation between the two plaintexts.

Since *CRISP* has a 128-bit block, the probability is vastly less than with 64-bit ciphers.

Resistance to attacks based on non-surjective round functions

An early version of the algorithm used four S-boxes in $S2()$. This produced a round function that was non-surjective (approximately 40% of the 2^{64} outputs were impossible). This led to the round function being theoretically vulnerable to an attack described by Bart Preneel in [3].

In practice, such an attack is unlikely to succeed, due to the very large tables that must be constructed, on the order of $2^{62.5}$ elements, or approximately 2^{65} bytes. Because the round-keys are 88 bits, even with a conservative estimate that the entropy is lower than the 88 bits suggested by the key size, an attack is also unlikely to succeed, even when enough table space is available.

CRISP was made substantially more resistant to this attack by the addition of a fifth S-box in the $S2()$ function, thus making less than 4% of the 2^{64} outputs impossible.

The performance penalty for implementing this was approximately 12.5%, with a 1K byte memory penalty.

Performance and Memory Requirements

The algorithm was implemented in C, using the GNU-C compiler on an HP-9000/735. The 6-round version produces an encryption rate of approximately 45,000 encryptions per second, or an equivalent data rate of 6.14Mbits per second. Using the native HP/UX compiler produces an approximate 4% performance improvement. There are opportunities for optimization; in particular, the S-box outputs may be composed with the $S2()$ function in a single table, reducing the number of table-lookups required in $f()$ by 30%.

The tables used to implement $ES()$, $S()$, and $S2()$ consume only 25K bytes of memory, which is easily within reach for a microprocessor/embedded controller implementation. The executable code on an HP9000/7XX system is approximately 3K bytes. Implementation complexity can be reduced by changing the key-scheduling algorithm to produce only the key-schedule elements, and dispense with key-dependance in the $S2()$ algorithm; the resulting cipher is then potentially subject to standard differential, and linear cryptanalytic attack.

Acknowledgments

The author gratefully acknowledges the patient tutoring, and expert advice of Carlisle Adams, both in the analysis of the *CRISP* algorithm, and in reviewing early drafts of this paper.

The author would also like to thank his management at *Nortel Technology* for allowing him to pursue topics that are only tangentially related to his main job.

References

- [1] J.A. Gordon, H. Retkin, *Are big S-boxes best?*, Lecture Notes in Computer Science nr. 149, 1983.
- [2] J. Lee, H. Heys, S. Tavares, *On the Resistance of the CAST Encryption Algorithm to Differential Cryptanalysis*, SAC '95: Workshop Record, pages 107-119.
- [3] Preneel, B., *On Weaknesses of Non-Surjective Round Functions*, SAC '95: Workshop Record, pages 100-106
- [4] E. Biham, A. Shamir, *Differential Cryptanalysis of DES-Like Cryptosystems*, Journal of Cryptology, vol.4, 1991, pages 3-72.
- [5] U. Blumenthal, S. Bellovin, *A Better Key Schedule for DES-like Ciphers*, paper to appear at PragoCrypt-96, September, 1996.
- [6] R. Rivest, *The MD5 Message Digest Algorithm*, published as RFC1321, April 1992.
- [7] B. Schneier, *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*, Fast Software Encryption, Cambridge Workshop Proceedings, 1994, pages 191-204.

Appendix A: Tables used in the *ES()* function

ES[0]

0x321, 0x4F7, 0x075, 0x720, 0x6B3, 0x199, 0x584, 0x52D,
 0x3CD, 0x1CB, 0x313, 0x1AA, 0x74E, 0x1E3, 0x465, 0x4C5,
 0x0F6, 0x478, 0x5F3, 0x364, 0x2F5, 0x420, 0x104, 0x3BC,
 0x00D, 0x754, 0x6E5, 0x103, 0x266, 0x070, 0x5C6, 0x03D,
 0x4EE, 0x3D7, 0x131, 0x033, 0x16A, 0x634, 0x027, 0x683,
 0x51E, 0x4DB, 0x2D9, 0x3D0, 0x615, 0x24D, 0x200, 0x119,
 0x30E, 0x0DA, 0x1D9, 0x028, 0x003, 0x561, 0x2C1, 0x121,
 0x157, 0x433, 0x168, 0x73A, 0x79B, 0x216, 0x0B5, 0x689,
 0x5FD, 0x365, 0x736, 0x4F8, 0x54D, 0x355, 0x242, 0x056,
 0x5AD, 0x552, 0x0AE, 0x388, 0x0D5, 0x288, 0x728, 0x4DD,
 0x700, 0x57D, 0x77F, 0x077, 0x5DB, 0x1BF, 0x204, 0x5B8,
 0x64C, 0x264, 0x424, 0x043, 0x67E, 0x03B, 0x586, 0x600,
 0x346, 0x359, 0x7B3, 0x150, 0x6E0, 0x5E9, 0x52C, 0x7AE,
 0x354, 0x3E5, 0x796, 0x102, 0x0F5, 0x471, 0x713, 0x182,
 0x304, 0x6D4, 0x4AD, 0x045, 0x513, 0x1EC, 0x466, 0x6C1,
 0x62C, 0x787, 0x2D1, 0x50B, 0x537, 0x6AD, 0x51C, 0x06D,
 0x4A6, 0x666, 0x0BA, 0x730, 0x187, 0x755, 0x106, 0x5D3,
 0x0BF, 0x20F, 0x5FA, 0x46F, 0x0C0, 0x147, 0x412, 0x590,
 0x208, 0x5D2, 0x65B, 0x694, 0x0B7, 0x314, 0x326, 0x7BA,
 0x721, 0x55C, 0x7A1, 0x3B7, 0x48C, 0x347, 0x217, 0x784,
 0x2C7, 0x42B, 0x3EB, 0x2D7, 0x28A, 0x1C6, 0x171, 0x3FB,
 0x3B5, 0x4E8, 0x703, 0x63C, 0x7A0, 0x7BE, 0x183, 0x70E,
 0x6D7, 0x776, 0x153, 0x2C6, 0x025, 0x41E, 0x0C8, 0x2D2,
 0x2BA, 0x049, 0x19D, 0x0EA, 0x4ED, 0x4DE, 0x606, 0x521,
 0x76F, 0x69B, 0x75C, 0x0D9, 0x08F, 0x56A, 0x558, 0x4AB,
 0x5EC, 0x7C7, 0x5DC, 0x4E2, 0x440, 0x7B7, 0x396, 0x42A,
 0x46C, 0x57B, 0x1C8, 0x6AF, 0x3B2, 0x4CB, 0x79A, 0x181,
 0x3A6, 0x107, 0x38C, 0x6E2, 0x038, 0x39C, 0x72A, 0x07E,
 0x302, 0x67F, 0x46E, 0x2B8, 0x4D7, 0x6B2, 0x320, 0x60D,
 0x400, 0x426, 0x509, 0x5D8, 0x716, 0x71D, 0x686, 0x3ED,
 0x15B, 0x00C, 0x6E1, 0x4BC, 0x202, 0x693, 0x41A, 0x67C,
 0x080, 0x571, 0x139, 0x21A, 0x469, 0x10A, 0x66E, 0x47F,

ES[1]

0x3E7, 0x638, 0x27D, 0x1B7, 0x05C, 0x46B, 0x68A, 0x54E,
0x1F8, 0x220, 0x392, 0x6F3, 0x010, 0x557, 0x0C2, 0x4AC,
0x230, 0x172, 0x7AA, 0x6A3, 0x1E0, 0x156, 0x3A2, 0x33A,
0x0A4, 0x5AB, 0x6D5, 0x14D, 0x2D3, 0x22E, 0x479, 0x589,
0x417, 0x303, 0x296, 0x773, 0x34D, 0x5F6, 0x712, 0x3FA,
0x130, 0x514, 0x3EF, 0x4E7, 0x627, 0x282, 0x342, 0x06A,
0x4BB, 0x1BA, 0x02C, 0x068, 0x46D, 0x1C7, 0x473, 0x29A,
0x2CE, 0x4C4, 0x47C, 0x457, 0x0FB, 0x48A, 0x7F3, 0x68F,
0x4B3, 0x7D0, 0x425, 0x0F7, 0x6B0, 0x7F2, 0x7E3, 0x437,
0x117, 0x02D, 0x1F6, 0x024, 0x7D4, 0x2D6, 0x40B, 0x682,
0x4B9, 0x6CA, 0x212, 0x02A, 0x546, 0x447, 0x5AF, 0x406,
0x12A, 0x791, 0x0E9, 0x461, 0x368, 0x613, 0x19A, 0x6DC,
0x20D, 0x43D, 0x261, 0x031, 0x43A, 0x175, 0x143, 0x50F,
0x44D, 0x00E, 0x247, 0x195, 0x470, 0x654, 0x72E, 0x0BD,
0x540, 0x489, 0x6AE, 0x2FB, 0x1B1, 0x408, 0x6CF, 0x268,
0x36F, 0x646, 0x07A, 0x621, 0x20C, 0x113, 0x2CD, 0x180,
0x297, 0x136, 0x31C, 0x7E5, 0x126, 0x252, 0x5F0, 0x53A,
0x662, 0x241, 0x58C, 0x54C, 0x405, 0x0A5, 0x62E, 0x642,
0x061, 0x43B, 0x243, 0x416, 0x7AC, 0x69E, 0x48D, 0x33D,
0x26A, 0x675, 0x246, 0x345, 0x42C, 0x40D, 0x57E, 0x36A,
0x286, 0x667, 0x178, 0x116, 0x3CF, 0x6FF, 0x725, 0x7D2,
0x4F9, 0x231, 0x752, 0x000, 0x04E, 0x6C2, 0x3FE, 0x0EE,
0x6E8, 0x160, 0x3DA, 0x002, 0x00F, 0x0CC, 0x765, 0x0FD,
0x3E8, 0x33B, 0x523, 0x1FD, 0x253, 0x448, 0x125, 0x5FE,
0x123, 0x65D, 0x1A4, 0x59F, 0x5C9, 0x743, 0x580, 0x4B4,
0x746, 0x04A, 0x041, 0x035, 0x45C, 0x510, 0x3AA, 0x63E,
0x7BC, 0x1DA, 0x610, 0x495, 0x3E4, 0x6BF, 0x2E8, 0x766,
0x22F, 0x16C, 0x573, 0x771, 0x6A4, 0x1B6, 0x6C4, 0x748,
0x5AA, 0x135, 0x047, 0x734, 0x096, 0x281, 0x1ED, 0x710,
0x43E, 0x42E, 0x4F3, 0x72B, 0x550, 0x607, 0x482, 0x2C2,
0x0D8, 0x7AD, 0x3E0, 0x4A9, 0x0AB, 0x744, 0x70C, 0x6AC,
0x1E4, 0x4E1, 0x014, 0x0B2, 0x305, 0x3F4, 0x4E5, 0x0F2,

ES[2]

0x3CE, 0x742, 0x37C, 0x24C, 0x037, 0x520, 0x643, 0x163,
0x2AC, 0x32B, 0x444, 0x0B0, 0x057, 0x6DB, 0x3F0, 0x77B,
0x23E, 0x0E4, 0x665, 0x0DD, 0x5D4, 0x167, 0x285, 0x086,
0x7F7, 0x79D, 0x0E5, 0x6F0, 0x032, 0x225, 0x016, 0x760,
0x711, 0x1F1, 0x23B, 0x36B, 0x753, 0x293, 0x2B3, 0x3BD,
0x7BB, 0x729, 0x576, 0x65C, 0x7FF, 0x08B, 0x386, 0x5B0,
0x3F9, 0x6D2, 0x04F, 0x309, 0x7CE, 0x3D8, 0x154, 0x1FE,
0x58F, 0x428, 0x76C, 0x0D1, 0x219, 0x27C, 0x1B8, 0x235,
0x769, 0x691, 0x5DF, 0x05A, 0x184, 0x52B, 0x394, 0x474,
0x731, 0x527, 0x329, 0x492, 0x5AC, 0x109, 0x647, 0x69D,
0x3D1, 0x31E, 0x58E, 0x18C, 0x30A, 0x575, 0x0D4, 0x5A3,
0x475, 0x556, 0x415, 0x361, 0x2DA, 0x2A5, 0x3B8, 0x59C,
0x02F, 0x48B, 0x749, 0x0BE, 0x6B4, 0x1F7, 0x38A, 0x36C,
0x13A, 0x4E4, 0x6CD, 0x052, 0x034, 0x380, 0x549, 0x6B9,
0x207, 0x55B, 0x639, 0x61F, 0x23F, 0x36D, 0x75D, 0x78A,
0x5E4, 0x528, 0x34B, 0x1B5, 0x525, 0x072, 0x52F, 0x740,
0x2CC, 0x4C8, 0x6FC, 0x4F5, 0x668, 0x16B, 0x3C0, 0x1BB,
0x705, 0x155, 0x089, 0x330, 0x4FA, 0x3C7, 0x690, 0x013,
0x22B, 0x1CF, 0x7DE, 0x419, 0x65F, 0x01B, 0x502, 0x18D,
0x1B9, 0x63B, 0x186, 0x4BE, 0x5EF, 0x2C5, 0x7A4, 0x7E2,
0x28E, 0x105, 0x257, 0x75B, 0x4B0, 0x62D, 0x158, 0x631,
0x3B6, 0x367, 0x17E, 0x1A7, 0x24A, 0x6DD, 0x1D2, 0x3D9,
0x3B3, 0x030, 0x40A, 0x6DE, 0x2CF, 0x2B1, 0x566, 0x4F6,
0x2E3, 0x09B, 0x723, 0x1F5, 0x1C0, 0x108, 0x007, 0x078,
0x69C, 0x0C3, 0x0FA, 0x5C3, 0x60B, 0x632, 0x0C4, 0x06B,
0x4A2, 0x7E0, 0x185, 0x0A9, 0x74D, 0x7F0, 0x0C7, 0x066,
0x1DE, 0x7EA, 0x64E, 0x53C, 0x322, 0x258, 0x53D, 0x5A2,
0x456, 0x376, 0x463, 0x2FC, 0x0AF, 0x3AC, 0x35B, 0x4CD,
0x67D, 0x477, 0x679, 0x114, 0x46A, 0x6E3, 0x08C, 0x12E,
0x4A5, 0x3F7, 0x357, 0x5EE, 0x209, 0x6BB, 0x533, 0x023,
0x61D, 0x567, 0x6CB, 0x19F, 0x3E1, 0x65E, 0x3F1, 0x671,
0x409, 0x005, 0x5C1, 0x389, 0x0D2, 0x2E9, 0x2F6, 0x6A8,

ES[3]

0x645, 0x198, 0x1E2, 0x61E, 0x508, 0x48F, 0x263, 0x0FE,
0x7DB, 0x7CA, 0x7C4, 0x536, 0x414, 0x308, 0x762, 0x228,
0x0AC, 0x2EF, 0x0D3, 0x379, 0x505, 0x73B, 0x588, 0x06C,
0x5E2, 0x69F, 0x1CC, 0x47E, 0x254, 0x59E, 0x5BA, 0x2DC,
0x411, 0x7E1, 0x3EC, 0x289, 0x1AD, 0x1AE, 0x5B7, 0x4F2,
0x34A, 0x74C, 0x17A, 0x44B, 0x381, 0x402, 0x6BC, 0x3C5,
0x553, 0x786, 0x33C, 0x413, 0x5A5, 0x38B, 0x5B6, 0x13C,
0x60C, 0x656, 0x190, 0x239, 0x617, 0x1E5, 0x3A9, 0x2A3,
0x79E, 0x6EB, 0x56E, 0x07F, 0x2E5, 0x1A9, 0x55F, 0x270,
0x094, 0x4FC, 0x063, 0x319, 0x017, 0x1DB, 0x59B, 0x2C9,
0x332, 0x66B, 0x06F, 0x73D, 0x23C, 0x5BC, 0x12B, 0x756,
0x248, 0x74B, 0x0D6, 0x763, 0x4EC, 0x7A9, 0x026, 0x32A,
0x38D, 0x076, 0x133, 0x3BA, 0x798, 0x1FC, 0x7D8, 0x661,
0x269, 0x6D3, 0x100, 0x2C3, 0x3DF, 0x144, 0x275, 0x01A,
0x07C, 0x391, 0x44C, 0x42D, 0x6CC, 0x7D6, 0x593, 0x0AA,
0x4D3, 0x6BE, 0x134, 0x26F, 0x73E, 0x4C9, 0x0E0, 0x3E6,
0x7FA, 0x3F3, 0x079, 0x779, 0x387, 0x1D6, 0x323, 0x676,
0x0E1, 0x71A, 0x77D, 0x499, 0x1C4, 0x120, 0x018, 0x287,
0x20E, 0x232, 0x476, 0x7D7, 0x1C3, 0x295, 0x45D, 0x66D,
0x4A1, 0x6C5, 0x24B, 0x1C5, 0x5C0, 0x6C7, 0x2A0, 0x0A0,
0x221, 0x40F, 0x2F4, 0x07D, 0x674, 0x544, 0x50E, 0x145,
0x1EE, 0x2D4, 0x542, 0x118, 0x1D3, 0x75A, 0x00B, 0x44E,
0x3D6, 0x112, 0x6BD, 0x5DE, 0x0CE, 0x2F3, 0x19B, 0x2DF,
0x481, 0x7C3, 0x35F, 0x5BF, 0x582, 0x34C, 0x71B, 0x17C,
0x626, 0x421, 0x49D, 0x79C, 0x35C, 0x4AE, 0x3A1, 0x1A2,
0x63F, 0x1D5, 0x5ED, 0x459, 0x71F, 0x3D4, 0x327, 0x715,
0x3FD, 0x020, 0x72C, 0x4E6, 0x768, 0x511, 0x15E, 0x581,
0x2B4, 0x350, 0x284, 0x625, 0x47A, 0x1D0, 0x7D3, 0x3FF,
0x065, 0x3C1, 0x403, 0x349, 0x616, 0x434, 0x6A0, 0x37D,
0x4D4, 0x563, 0x2BE, 0x32C, 0x56D, 0x60E, 0x274, 0x3C6,
0x76B, 0x7A6, 0x6FA, 0x05B, 0x236, 0x529, 0x5A1, 0x1A3,
0x2C4, 0x240, 0x61B, 0x652, 0x57A, 0x3A4, 0x398, 0x2F0,

ES[4]

0x298, 0x36E, 0x5D9, 0x7DA, 0x0F8, 0x0FF, 0x161, 0x767,
0x78F, 0x5E0, 0x21E, 0x699, 0x3AE, 0x358, 0x574, 0x707,
0x7DF, 0x362, 0x506, 0x7B6, 0x6B1, 0x2B6, 0x352, 0x3A5,
0x18F, 0x61A, 0x0A3, 0x197, 0x13F, 0x7A5, 0x611, 0x41C,
0x78E, 0x5D7, 0x265, 0x2F7, 0x4C2, 0x22A, 0x3CC, 0x678,
0x09E, 0x334, 0x3B4, 0x498, 0x3AD, 0x5F7, 0x1FF, 0x2E7,
0x09A, 0x487, 0x44A, 0x7E9, 0x1D8, 0x5A7, 0x7C1, 0x5D6,
0x2EA, 0x062, 0x3BE, 0x622, 0x083, 0x592, 0x7E6, 0x7E4,
0x37B, 0x0DC, 0x793, 0x562, 0x249, 0x78C, 0x360, 0x5F4,
0x5DD, 0x5B5, 0x431, 0x1FA, 0x6A7, 0x612, 0x312, 0x789,
0x18B, 0x59A, 0x30B, 0x443, 0x159, 0x2D8, 0x602, 0x7D1,
0x2CB, 0x11F, 0x608, 0x4EB, 0x02B, 0x486, 0x1C1, 0x5C5,
0x092, 0x087, 0x62A, 0x2ED, 0x775, 0x49F, 0x623, 0x68D,
0x1A0, 0x3C2, 0x162, 0x40C, 0x341, 0x442, 0x452, 0x709,
0x2AA, 0x27A, 0x09D, 0x374, 0x438, 0x517, 0x28D, 0x7A7,
0x331, 0x472, 0x2A7, 0x324, 0x18A, 0x5BE, 0x2CA, 0x0B6,
0x00A, 0x449, 0x5E7, 0x255, 0x423, 0x371, 0x564, 0x3BB,
0x29B, 0x738, 0x790, 0x5CA, 0x74F, 0x082, 0x33E, 0x53F,
0x122, 0x51D, 0x363, 0x697, 0x6C6, 0x629, 0x504, 0x601,
0x1EB, 0x6D6, 0x343, 0x2B2, 0x7F5, 0x64F, 0x450, 0x0BB,
0x3F8, 0x11C, 0x03F, 0x036, 0x6DF, 0x193, 0x044, 0x08D,
0x491, 0x5FF, 0x1DD, 0x26C, 0x2C8, 0x6CE, 0x44F, 0x26E,
0x783, 0x5B4, 0x6B5, 0x3A3, 0x4B2, 0x03E, 0x7B1, 0x233,
0x585, 0x5E3, 0x6E4, 0x5EB, 0x3E3, 0x2A1, 0x706, 0x6C9,
0x0CA, 0x01E, 0x5B3, 0x201, 0x0C5, 0x353, 0x458, 0x770,
0x009, 0x15F, 0x37F, 0x55D, 0x17F, 0x1F2, 0x262, 0x49C,
0x56F, 0x526, 0x250, 0x29F, 0x7C2, 0x0CF, 0x6D8, 0x13D,
0x073, 0x29E, 0x6FE, 0x4E0, 0x501, 0x7E7, 0x20A, 0x0B3,
0x788, 0x560, 0x6D9, 0x6E9, 0x4D5, 0x543, 0x50D, 0x1BC,
0x21C, 0x11B, 0x4CC, 0x0F1, 0x72D, 0x722, 0x635, 0x3A0,
0x596, 0x727, 0x0F4, 0x545, 0x772, 0x650, 0x75E, 0x1E9,
0x4EF, 0x64B, 0x483, 0x234, 0x56B, 0x4A4, 0x7C9, 0x70F,

ES[5]

0x39D, 0x757, 0x733, 0x05F, 0x5B9, 0x22D, 0x03A, 0x445,
0x58B, 0x18E, 0x5CC, 0x370, 0x188, 0x0A6, 0x2AE, 0x55E,
0x4D2, 0x229, 0x1A5, 0x67B, 0x140, 0x317, 0x39E, 0x1AF,
0x7FD, 0x692, 0x27E, 0x348, 0x6A2, 0x58A, 0x522, 0x1DC,
0x351, 0x49A, 0x609, 0x344, 0x2E1, 0x060, 0x3A7, 0x468,
0x446, 0x4B6, 0x1A8, 0x4E3, 0x191, 0x318, 0x04C, 0x16D,
0x110, 0x245, 0x4D9, 0x299, 0x435, 0x15D, 0x6C0, 0x294,
0x4C3, 0x7CC, 0x5D0, 0x222, 0x3F5, 0x042, 0x214, 0x10B,
0x441, 0x32D, 0x4D1, 0x3F6, 0x4AA, 0x5E6, 0x5F5, 0x04B,
0x5AE, 0x256, 0x70A, 0x378, 0x76D, 0x71C, 0x338, 0x792,
0x799, 0x2DE, 0x77A, 0x4BF, 0x15C, 0x427, 0x05D, 0x16F,
0x7EC, 0x570, 0x619, 0x5CD, 0x4CF, 0x47D, 0x68E, 0x54B,
0x325, 0x2A8, 0x10D, 0x02E, 0x2E2, 0x794, 0x451, 0x021,
0x52A, 0x7D9, 0x1EF, 0x660, 0x09F, 0x6ED, 0x148, 0x17D,
0x66F, 0x64A, 0x099, 0x278, 0x6AB, 0x644, 0x290, 0x211,
0x051, 0x393, 0x26B, 0x356, 0x719, 0x271, 0x279, 0x5A6,
0x7FC, 0x6FB, 0x63A, 0x436, 0x559, 0x366, 0x382, 0x1CA,
0x384, 0x3E9, 0x3D2, 0x4C7, 0x735, 0x1F9, 0x2BC, 0x277,
0x42F, 0x04D, 0x4F0, 0x45A, 0x170, 0x782, 0x410, 0x500,
0x15A, 0x395, 0x38E, 0x244, 0x4A3, 0x677, 0x32F, 0x138,
0x3DC, 0x203, 0x30D, 0x591, 0x685, 0x56C, 0x58D, 0x3F2,
0x572, 0x778, 0x3C9, 0x3CA, 0x2FF, 0x3D3, 0x4DA, 0x60A,
0x316, 0x1B4, 0x5CE, 0x532, 0x535, 0x055, 0x555, 0x0F3,
0x40E, 0x069, 0x2DB, 0x276, 0x25C, 0x1E7, 0x701, 0x6F1,
0x696, 0x137, 0x2D0, 0x653, 0x774, 0x432, 0x603, 0x169,
0x1E6, 0x1E8, 0x7EB, 0x6F5, 0x0B1, 0x097, 0x684, 0x418,
0x1F3, 0x37E, 0x399, 0x63D, 0x74A, 0x6FD, 0x45B, 0x651,
0x7A2, 0x3DD, 0x23A, 0x012, 0x19E, 0x79F, 0x095, 0x4A7,
0x2D5, 0x2B5, 0x630, 0x6F8, 0x085, 0x5C4, 0x69A, 0x2AF,
0x618, 0x624, 0x218, 0x273, 0x3EA, 0x101, 0x12F, 0x485,
0x6F6, 0x28B, 0x5BB, 0x046, 0x698, 0x702, 0x127, 0x6D0,
0x10C, 0x3CB, 0x3AB, 0x695, 0x040, 0x7B9, 0x6E7, 0x31F,

ES[6]

0x1D4, 0x29C, 0x76A, 0x377, 0x1E1, 0x1AB, 0x578, 0x071,
0x78D, 0x4FF, 0x5E5, 0x6F4, 0x35D, 0x22C, 0x383, 0x315,
0x32E, 0x4BA, 0x657, 0x20B, 0x7BD, 0x407, 0x11A, 0x4D0,
0x41F, 0x7C8, 0x568, 0x21B, 0x726, 0x714, 0x530, 0x7B4,
0x35E, 0x541, 0x49B, 0x19C, 0x14B, 0x745, 0x6EE, 0x7FE,
0x780, 0x1A6, 0x57F, 0x66A, 0x7E8, 0x01F, 0x5A9, 0x538,
0x6B7, 0x7B0, 0x614, 0x098, 0x670, 0x2F9, 0x019, 0x4FE,
0x4FD, 0x3BF, 0x5B1, 0x708, 0x6F7, 0x7F8, 0x283, 0x34F,
0x718, 0x1F4, 0x0D7, 0x27F, 0x0EF, 0x2EE, 0x339, 0x637,
0x2F8, 0x06E, 0x583, 0x587, 0x260, 0x251, 0x597, 0x0A7,
0x206, 0x291, 0x60F, 0x54F, 0x280, 0x129, 0x7B5, 0x43C,
0x194, 0x205, 0x3DE, 0x430, 0x6E6, 0x2A6, 0x2FD, 0x512,
0x173, 0x165, 0x3EE, 0x518, 0x659, 0x093, 0x1C2, 0x301,
0x737, 0x565, 0x4CA, 0x77C, 0x25A, 0x4F1, 0x6EA, 0x460,
0x5F8, 0x189, 0x091, 0x35A, 0x39B, 0x649, 0x2F2, 0x310,
0x27B, 0x272, 0x21F, 0x62F, 0x66C, 0x0E3, 0x49E, 0x704,
0x7DC, 0x084, 0x6A1, 0x369, 0x2EB, 0x797, 0x658, 0x174,
0x78B, 0x5D5, 0x4B8, 0x5FC, 0x62B, 0x5E1, 0x655, 0x664,
0x11E, 0x669, 0x72F, 0x0A2, 0x688, 0x59D, 0x50A, 0x496,
0x628, 0x081, 0x0C6, 0x6B8, 0x5A0, 0x292, 0x50C, 0x51A,
0x493, 0x641, 0x6A6, 0x38F, 0x2AD, 0x77E, 0x1BD, 0x1EA,
0x6DA, 0x306, 0x7CF, 0x124, 0x1D7, 0x2BF, 0x4AF, 0x0E7,
0x149, 0x45F, 0x6D1, 0x3D5, 0x422, 0x115, 0x11D, 0x577,
0x5B2, 0x16E, 0x4E9, 0x73C, 0x595, 0x0DE, 0x0DB, 0x3B9,
0x7B8, 0x43F, 0x0FC, 0x484, 0x1B3, 0x51B, 0x372, 0x5F1,
0x6A5, 0x14E, 0x6F9, 0x717, 0x7AB, 0x7BF, 0x6A9, 0x7AF,
0x31A, 0x4C6, 0x029, 0x7F4, 0x2DD, 0x01D, 0x747, 0x795,
0x4B5, 0x455, 0x61C, 0x152, 0x76E, 0x2BB, 0x1FB, 0x5C2,
0x0B4, 0x08A, 0x7F6, 0x73F, 0x429, 0x604, 0x064, 0x75F,
0x1B2, 0x25D, 0x6F2, 0x3C8, 0x0DF, 0x5E8, 0x4BD, 0x13B,
0x3FC, 0x215, 0x4D6, 0x3C3, 0x6EF, 0x12D, 0x751, 0x0B9,
0x1DF, 0x3C4, 0x397, 0x267, 0x2FE, 0x7C6, 0x68C, 0x663,

ES[7]

0x7ED, 0x48E, 0x4DF, 0x09C, 0x07B, 0x4EA, 0x65A, 0x0C1,
0x5F2, 0x724, 0x1AC, 0x004, 0x0BC, 0x3B0, 0x1F0, 0x0EB,
0x515, 0x633, 0x238, 0x2BD, 0x1D1, 0x761, 0x3E2, 0x25E,
0x14F, 0x328, 0x488, 0x490, 0x337, 0x058, 0x7FB, 0x039,
0x1C9, 0x048, 0x23D, 0x224, 0x177, 0x192, 0x57C, 0x758,
0x2E4, 0x6AA, 0x497, 0x764, 0x503, 0x777, 0x0B8, 0x2B0,
0x3DB, 0x648, 0x213, 0x551, 0x0A1, 0x598, 0x336, 0x227,
0x33F, 0x0ED, 0x454, 0x022, 0x785, 0x151, 0x0EC, 0x680,
0x5C8, 0x13E, 0x41B, 0x605, 0x67A, 0x2C0, 0x759, 0x687,
0x03C, 0x5BD, 0x237, 0x2EC, 0x739, 0x050, 0x404, 0x480,
0x5A4, 0x223, 0x70B, 0x0C9, 0x7A3, 0x439, 0x335, 0x47B,
0x24E, 0x375, 0x14A, 0x453, 0x464, 0x05E, 0x31B, 0x30C,
0x3A8, 0x01C, 0x166, 0x6EC, 0x2A2, 0x4C1, 0x519, 0x10E,
0x0CB, 0x0AD, 0x132, 0x6C3, 0x074, 0x259, 0x333, 0x51F,
0x548, 0x5C7, 0x25B, 0x0E2, 0x0E8, 0x547, 0x7CD, 0x53B,
0x5A8, 0x0CD, 0x507, 0x41D, 0x1CD, 0x52E, 0x210, 0x390,
0x37A, 0x300, 0x64D, 0x534, 0x28C, 0x594, 0x2E0, 0x70D,
0x176, 0x539, 0x4B1, 0x579, 0x781, 0x1BE, 0x569, 0x0A8,
0x373, 0x4F4, 0x7EE, 0x226, 0x340, 0x08E, 0x2B9, 0x599,
0x45E, 0x4C0, 0x34E, 0x640, 0x53E, 0x179, 0x31D, 0x1B0,
0x7F9, 0x7C0, 0x2FA, 0x5DA, 0x2AB, 0x2B7, 0x0D0, 0x524,
0x0F9, 0x26D, 0x531, 0x462, 0x68B, 0x516, 0x0F0, 0x681,
0x090, 0x0E6, 0x3AF, 0x5F9, 0x55A, 0x620, 0x12C, 0x4D8,
0x4B7, 0x30F, 0x401, 0x71E, 0x5FB, 0x128, 0x7C5, 0x7DD,
0x732, 0x672, 0x7CB, 0x7EF, 0x14C, 0x4CE, 0x17B, 0x008,
0x2E6, 0x015, 0x5CF, 0x2A9, 0x6B6, 0x7F1, 0x053, 0x467,
0x750, 0x141, 0x088, 0x1CE, 0x4FB, 0x006, 0x24F, 0x142,
0x10F, 0x5EA, 0x673, 0x28F, 0x54A, 0x059, 0x494, 0x3B1,
0x7B2, 0x196, 0x011, 0x311, 0x554, 0x307, 0x054, 0x2F1,
0x25F, 0x6BA, 0x741, 0x5CB, 0x001, 0x39F, 0x636, 0x164,
0x385, 0x4A8, 0x111, 0x067, 0x7D5, 0x39A, 0x1A1, 0x21D,
0x2A4, 0x5D1, 0x6C8, 0x4DC, 0x7A8, 0x29D, 0x4A0, 0x146,

Appendix B: Example Tables used in $S()$ function

S[0]

7, 69, 15,248,179, 22,125, 84,192,153,103,188,252,126,214,177,
 146,208,246, 36,212,243, 92, 73, 87,171,255,238,197,205,196, 86,
 100,118, 32,164, 44,222,203,183,245, 59,178,127,206,158,137, 18,
 65, 1, 72,162, 11,109, 56, 45,216, 42, 37,211, 43,198,140, 48,
 64, 50,220,123,170,119,157, 58, 31,156,155, 82,139,152,174,175,
 35,237, 54, 4,166, 71,190,186, 53, 41, 2,213,110, 26,151, 55,
 235, 74, 12,136, 0,241,236,226,182,111, 24, 33, 96, 16, 97, 6,
 204, 75,104,113, 8,107,176,217, 23,233,121,130,191, 17, 81,120,
 38,225,161, 14, 19, 40,231,201, 39, 9,114,165, 89,210, 3,150,
 145,115, 99,187, 30, 61,122, 63, 25, 95,209,168,230,106, 62,105,
 102, 98,227,247,135,189,138,219,112,240,215,234,144, 90,202,132,
 134,154,148,254, 76,224,117, 93,116,253,108,195, 13, 51, 21,239,
 249, 46,133, 66,129, 83,223,221,173,141,169,180, 78, 94, 88,142,
 85,244,194,128,149,184, 49,159,218, 77, 52,185, 91, 68,251,232,
 124, 29,207, 57,242, 60,172, 10, 20,250, 67,101, 79, 47,228,200,
 34,163, 28,199,131,193, 80,167, 70, 5,229,147, 27,143,160,181,
 182,117,173,103, 93,114, 61,197,112, 54,151, 13,242,160,189,157,
 17,218, 2,156,213, 69,249,120,166,145,226,206,154, 56,123, 47,
 202,138, 65,207,245, 66,192,158,221,220,136,191,187,107, 16,208,
 199,105,210, 88,143, 27, 62,200,195,193, 64,101, 99,230,104,178,
 44,106,172,102,250,180,229, 3, 10,125,228,142,161,225, 9, 75,
 96, 94,167,233,164,240, 60,209,212,248,141,241,194,204, 97, 78,
 140, 57, 5,247, 28, 31, 39,133,146,224, 53,217, 43,134, 92,237,
 188, 21, 42, 77,227, 35,203,252,147, 45,190,223,246,251, 51,234,
 89, 11,219,214, 87, 34,122,170, 26,155, 36,118,183, 18, 58,132,
 6, 30,239, 22, 46,231,236, 95, 55, 76,130,111,184, 67, 72,150,
 59,109,116, 48, 7, 83, 23,222,137, 86,169, 70,139,238, 74, 12,
 186, 85, 20,127,126,175, 50, 68,119,148,185, 81, 4,162,253,171,
 159,196, 33, 90,165,176,216,110, 63, 29,135, 15,179,149,181, 37,
 255, 91, 24,211,152, 1,100,129,168, 25,144, 19,198, 40,108,174,
 128,113, 0,153, 98,254,163,215, 80, 32,244, 14,205, 73,232, 49,
 243,124, 38,121,115, 71, 82, 8,177,235, 84, 41, 52, 79,131,201,
 230,143,138, 42, 16,180,114,118, 15, 51, 1, 19,228, 35, 37,171,
 247,206,199,211, 18,227,192,224, 92,225,176,112,160, 36,168,119,
 65,129,198, 50,231,173, 93, 81, 3,135,102,155, 26,248, 48, 74,
 146, 25, 63,195, 54,216,200, 69,133,217, 2,240,101, 53,104, 90,
 109, 77,191, 98,233,183,163, 72,106,196,246,166,126,208, 43,148,
 136, 99, 44,252,210,236, 61, 28,120,113, 34,132, 67,110,177,122,
 185, 57,139, 23,197,218, 9, 52, 46,144,194, 94,182, 32, 8, 79,
 123, 86, 29, 5,153,179,157,165,145, 13, 49,190, 4,184, 21,189,
 186, 78, 95,243,241,103, 30,254, 71, 39,237, 73,105,121,151, 76,
 149,204,232, 20, 62, 41, 70,158, 97,221,130,167, 84,181,162,202,
 47, 40, 14, 89,150,229, 24, 58,212,203,250,159, 55,174,134,234,

91,219, 11,215, 88,124, 59, 22,154,140,156,214,207, 80,244,161,
108,205, 27,116, 17, 85, 10,137, 60,147, 83,169,115,128,253,239,
117,245,188,107,172, 0,127, 96,209, 66, 31,238,141,125,193,100,
164,249,170,220,187, 75,178,131,152,242, 68,255, 33, 56, 87,213,
175, 12,235, 7,142,251,201,223, 6,222, 64,111, 82,226, 45, 38,
52,178, 4, 75,122, 43,249, 49, 25, 7,148,227, 31,124,201,205,
171,101,165, 18,240, 82,158, 9,144,127, 71, 40,156,141,233,206,
187, 38,199, 95,239,105, 78,138,116, 97,225, 59,151,195,140,168,
157,145,253, 19,196,179, 65,150,136, 80, 42,254, 44, 32,137, 37,
132, 16, 66,197,247, 6,170,119, 28, 57,160, 73,243,216,198,220,
153, 79,188, 47, 50, 92,106, 15,251, 53,180, 1,111,113, 89,175,
204, 70, 45,224,112, 64,238,128, 63, 60, 91,110,219,223, 21,107,
121,215, 76, 13, 3,241,115, 10, 86, 88,129,221,114,169, 94,149,
24,183,250, 12,126,109,177, 74, 2,211,189,228,203, 54, 0, 69,
34,133,147,190, 77,100,139,214, 55,135,181,161, 83, 8,172,231,
143,103, 26, 99, 46, 22,230, 27, 90, 29,163,207, 72, 87,146,104,
232,184,176, 84,202, 5, 48,194, 20,191, 62,166,152,248, 35,131,
61,182,229,245,244,154,234,130,134,218, 17,162, 56,108, 85, 23,
36,252, 67,213, 30,212,208, 81,118,226,217,209, 41,142, 14,185,
237,242,125,167,210,235, 33,123, 68,200,246, 51, 96,255,236,120,
173, 39,193,164, 58, 11,117,102, 98,222,159, 93,155,192,174,186,
122,142,100, 45, 70,124, 30,138, 59, 71,214,191,204,180, 39,168,
120,215, 53,146,131, 76,237,192,144,213, 64, 90, 8,143, 88,159,
207,104, 14,241,234, 18, 74, 60, 20, 80,161, 10, 96, 41, 69,210,
55, 32,229, 85,115, 99,251, 79, 62,254, 52,127,106,243, 93,177,
255, 49,182,197,230, 2, 57,128,132, 42,245,193, 43, 98, 66,238,
82,231, 58, 24, 31,224,226,165,154,164, 87,103, 11,221, 54,201,
160, 33,126, 17,206,208,114,109,152, 44,233, 25,163,137,205,119,
35, 4,116, 46,186, 3,158, 5,202, 84, 15,123,242,189,101,248,
134,194, 19, 37, 36, 72,113, 6, 26, 50,112,171,117,157, 0,185,
92, 27, 13,218, 56,211,110, 47,170,175,162,166,135,188,156, 28,
139,102,125, 1,149,249, 7, 21,227,216,181, 75,244,199,107,190,
130, 65, 81,187, 40,200, 86,176,196,108, 34,147,203,236, 94, 22,
169, 9,145,153,174, 63,150,136, 12,223, 78, 73, 68,235,129,247,
195, 29, 97, 23, 77, 48,246, 61,240, 51,212,172,217,232,252,140,
141,178, 38,173,118, 89,105,219,151, 95,198, 91, 16,184, 67,228,
111,133,220,121,222,155,148,167,239,183,253,225,209,250,179, 83,
198,219,161,229, 41,120, 50,107, 78,165,121, 74,153, 46, 70,177,
189,170,240,245,112, 63,191,235, 80, 85, 7, 40, 31,154, 51, 11,
221,181,163, 24, 57,195,186, 97,124, 23,246, 95, 9,110, 61, 58,
187, 84, 30, 5,251,131,207,243,166, 93, 48,117,185, 2,150,160,
68,239,142, 15,202,139,138,100,173,172, 42,216,194, 43,244,206,
180, 98,141,184,233, 82,155, 16, 72, 87,228,122,114, 10,116, 47,
169, 91,132, 52, 25,109, 77,190,136,171,188,119,242, 34, 45,108,
167,215,203,223, 27,101,149, 14,128,210,234,126, 96,225, 0,208,
123,205,254,175,226, 44, 29,182,231,238,143, 37,179, 1,193,174,

211, 3, 54, 65, 90, 8, 19,144,249,115,237,209,204,212,255, 38,
 134, 53,248,218,230,113, 17, 69, 92, 94, 71,222,241,146,145, 75,
 6,111, 36,104,164,147, 39,250,199,135,162,196,217,156,103,130,
 140, 89,220, 21,183, 59,148,227,159,151,178,192,127,102, 76,168,
 214, 12,118, 81,137, 32,129, 4, 56, 33, 35, 62,252,152, 26, 22,
 67,213, 73, 66,133, 88, 28,232,157, 99, 79,158,224, 49, 60, 13,
 106, 20,253, 55, 86,201,236, 18, 64,125,176,197, 83,105,200,247,
 25,213,125,106,183, 54, 93,142,191, 23,173,197, 6,113, 3,244,
 16,240, 20,175, 30,215,161,205, 32, 31, 19,243, 62, 70,107, 87,
 42, 75, 39,168, 9, 24, 74,188,121,163,218,111,211,145,251,234,
 73,120,139,236,221,143,127,138, 91, 40,128, 63, 14,124, 37, 26,
 36, 81,104, 7,112, 98, 68, 52, 51,101, 71,194,239,230,147,102,
 159,238,169,184, 66,105,231,228, 47, 18,178, 80, 82, 8, 49,232,
 79,190, 88,167, 45,226, 50, 27,193,141,150, 72,129,219,174, 35,
 41,222,154, 65,166, 58,237,212, 38, 96,133,122,135,235,103, 34,
 248,144, 17,200,118,204, 29, 64,149,201,223,187, 13,246,162,225,
 97,171, 77,137, 22,189,176,233,119, 67,114,160, 15,151,115,109,
 153,116,134,203, 60,172,117,131, 43, 4, 83,186,179, 56, 28, 53,
 108,156,254,136,217,207,170, 92, 61, 46,155, 90, 86,126, 11,195,
 148,227,140,110,252,130,209, 5,216,242,250,198,164,192,181,255,
 146,247, 89,206, 85,100, 94, 2,253, 69,177, 84,208, 76,165, 59,
 95, 10, 21,152,132, 55,249, 12,214,202, 99,241, 44,229, 48, 1,
 78,210,199,224,245, 0, 57,180,185,123,182, 33,157,220,158,196,
 139, 90,188, 83, 69, 3,102,221, 64, 31, 41,207,136,179,240, 66,
 211,168, 72, 91,251,108,232, 92,161,128,225, 8, 50, 14,193,115,
 95, 53,190,159,103,104,246, 51,165,241,113, 37,204, 7,167,224,
 17,176,100,122,208,196,111,194,178, 59,205,133,119,174, 5,222,
 201,236,235,219,162,116,212, 28, 42,169,192,147,210, 26,197,137,
 245,209, 98,252, 52,172, 23,107,117, 4, 63, 49,216, 82, 60,112,
 200, 27, 19, 20,234,153,180,130, 44,101, 33, 71,195, 67,255,250,
 129, 22,244,134, 84,106,238, 36,141, 15,181,163, 9,145,214,155,
 55, 46,237,166,170, 35,140, 78,186, 76,173, 18,185,156,150,198,
 217,242, 0,120, 97,175,199, 47,226,227, 56, 12,220,187, 85, 68,
 62,183,191, 40,160,158,127, 39,249,206,184,114,203,154,239,151,
 30, 81,138,164, 1,157, 10,123,146, 48,132,135,215,144, 94,152,
 109, 93, 70, 77, 74,254,126, 87,177, 79, 80,142, 99,143, 29, 11,
 32,110, 89,118,125,248, 16, 86,243,182, 6,189,124, 88,171, 61,
 231,148,149, 73,228, 38,218, 43, 75, 2,223, 65, 57,213, 13, 34,
 131,247, 58, 45,253, 24,105,229,121,202,233, 25, 54,230, 21, 96,

S[1]

250, 9, 47,157, 57,118,152, 66, 54,160,140,127,197,213, 92,222,
108,193,200,134, 12, 90, 41,218,175,102,189,168,162,207, 36,109,
124,242,121, 52, 86,209, 76,163, 91,132,215,195,243,199,174,116,
165,106, 43,221,226,133,217,223,153,103,119, 30,172, 95, 35, 94,
248, 38, 88, 89,249,188,181, 0,184, 48, 29,148, 5,241,232, 84,
114, 33, 26,220,178, 51, 11,211, 61, 83,120, 40,144,143, 60, 73,
171,151, 77, 20,141,146,228,161, 96, 68,115,126, 13,202,251, 45,
34,180,154,131,244, 80, 32,149,138,237, 14,167, 50, 16,158,185,
78, 85,247, 10, 82,176,182,139, 25,210, 17, 39,252, 98,128,183,
239, 56,159,238,110,187, 15,230, 31, 21, 81, 22,229,142,227, 87,
111,205, 24, 64, 6,233, 53,104,254, 44,255,170,224, 58,155, 97,
79,236, 72,204, 3,192,123, 46,112,219,136,105, 49, 67, 23,164,
27,100,245,196, 63, 18, 99, 69,173,169,203, 74, 93,137, 7,206,
208,198,190,129,235,150,117, 75,147, 65, 71,107,125,156,101,212,
179,113, 28, 59, 42, 62, 55,122,246, 37,231,216,130,194,177, 1,
8,166, 19,240,234,253,225,191,186, 2,145,135,201,214, 4, 70,
114, 23,176,151,212,111, 79,199,116,254,146, 82,172, 39,118,211,
22,152,108, 47, 0,204,180,255,222, 37,240, 73,213,250,134,216,
189,175,162, 12,161,126, 66,220, 83, 89,223, 81,227,235,191,182,
138, 90, 26,102, 51,166,253,137,239,196,214,170, 72, 96, 3, 8,
86,217, 49,224,185, 41, 2,202,244,104,135, 95,100,107, 80,243,
231, 19,229,228,249,145,179, 42, 9,130, 84,168, 15,177,219, 88,
142,187,234,105,209, 67, 59, 93,106,215,190,103,169,174, 38,245,
147,230,127,247,131,122, 48, 30, 52,201, 31, 7,129, 56, 70, 13,
69,141,206, 35,160,194, 32, 76,121, 54,155,153,188, 43,246,203,
150,115, 60, 46,101,238,195, 94,112, 17,133, 65, 92,164,158,210,
33,154,125, 87,181, 34,156, 27, 77,241,144,159,248,149,167, 45,
178,207, 64,205, 99,173, 20, 21, 25,113,136,139,197,218, 40, 4,
91, 78,192, 29, 18,225,163, 68,140,183, 24,128,193, 36, 61,198,
208, 58,242,109, 62,226,236,117, 1, 5,157,143,148, 98, 50,165,
124,120,251,110, 28,171, 63, 85,119, 57,232,252, 55, 14,186, 10,
71, 97, 16,132, 6,237,184, 75,123,221, 11,233, 74,200, 44, 53,
188,225,119,123,161,200,182,192,109,164,131,242, 21,205, 88, 84,
124,145, 32,112, 14, 66,178,128, 96,243, 25,195,213,194, 46, 40,
79, 72,154,116,169, 93,172,233, 34,130, 87,115, 18,249, 38, 30,
121, 90, 77, 3,135,138,214, 62,176, 50, 98,160, 43, 7,228,126,
15,250,193,210, 23, 2,107,199, 82, 29,113, 10, 64, 81,137, 37,
65,159, 4,120, 71, 68,224, 89,207,235,132, 75, 33,142, 20, 49,
95,170,150,220,241, 39, 78,184,185,146, 41,171,156,186, 5, 44,
80, 17, 42, 0,133,197, 97,244, 76, 94, 13, 45,219,105, 86, 6,
122,117, 61,218,175,118, 57,232,139,191,245, 24,153, 51, 59,179,
155, 52,158, 55,140,253,201, 67, 99, 85,189,255,212,209,237, 58,
28,236,216,198, 92,238,114, 12, 53, 1,203,148,111, 73,108,202,
177,101,127,125,162,231,166, 9,246,141, 74,208,129,240, 63,100,
70, 69, 54, 60,226,223,252,168,234,157,134,174, 11,149,248, 22,

196, 35,215, 91,217,151,183,167,221, 56,144, 16, 19,206,222,211,
230,103, 47, 36, 8, 26,136,143,187,152,229,251,173,163,204,190,
180,102, 83,227, 31,104,106,147,165,110, 48, 27,181,239,254,247,
242,102, 26,105,129, 96, 66,179,141,136, 20,226,142,255,205, 75,
30, 57,117,153,126,227,213, 85, 21, 43,110,203,108,121,104,176,
47,237, 0,201,215,159,168, 59,248, 70, 88, 89, 40,219,194, 61,
241, 36,206,130, 33,217,209, 87, 83,204,220, 64, 11,133,222,144,
158, 9,196,251,230, 82, 42,225, 80, 54,207,116, 93,134,229, 58,
211, 35, 72, 73, 81,239, 18,174,184, 62, 77,200, 22, 79, 32, 99,
17,111,162,223,173, 48,185,135,171,232,208,164,224,188,115, 39,
247,186, 71, 41, 28,148,167,212, 44, 16, 53, 38,143,218,109,202,
163, 4,189, 23,249, 19,169,120,216,235, 51, 15,139,127,106, 6,
31,137,101,175, 34, 2,236,180,165,192,155,246,150,245, 63, 65,
50, 91,177,191, 3, 97,123, 46, 45,254, 12,149,151, 76,160,233,
1,199,112, 78, 37,214,195,181,253, 8, 7,118,132,131, 69,138,
146,172,250, 5, 60,187,128,234, 24,190, 74,113, 14,166, 92,182,
161, 49,124, 52, 25,238,231,170, 55,244, 68, 90, 56,152,125,122,
119, 10,157, 95, 84,147,154,228,193,240, 27,107, 13,210, 29,252,
178, 86,197,198,114,183,156,145, 67,103,140,243, 98, 94,100,221,
49, 70, 15,238,124,213,242,132,211,143,177, 18, 39, 13,170,105,
23,235, 83, 76,165,117,147, 52,161,202, 44,203,151, 64,106,126,
14, 45,186, 46,163, 71, 99,168,158, 51,173,121,118, 75,199, 22,
204, 7,216,209,201,160, 27,148,144,116,102, 59,190,233,223,129,
33,249, 12, 67, 1, 34, 36,156,193,123,248, 0,136, 11,184,113,
245, 69,139,176, 97,225,236,153,246,191,159, 57, 47,101,220,205,
119,169,251,130,104, 41,227,247,171, 95,196, 3,114,152, 96,162,
74, 81,133,150,134, 2,127,103,125,240, 68,230, 8,214, 20, 19,
37, 38,128,182,155,197,215,254,208,210,174, 28, 29, 16, 80,250,
198, 65,131,146, 88, 48, 26,221,178, 30, 63,218, 24, 6, 25,164,
219, 84,237,212,157,222,138,120, 94,252,255, 60,112,149,207, 43,
253,192, 91, 50,145,100, 73,166,181, 61, 32,229, 35,122,179,194,
137, 21, 10, 5,206,243,188, 86,185, 53, 62,187, 85,234,228,195,
31,135, 90,107, 42,231, 72, 4,142, 40,154, 56,109,224, 89,172,
175,239,241,244, 58, 55, 93,110,183, 66, 87, 92, 82,232, 54,189,
167, 9,115, 77,108, 17,180,226, 78, 98,217,140,200,111,141, 79,
90,177,128, 59,159,211, 56,119, 11,174,143, 94, 1,102, 85, 54,
63,246,233,230,203,139, 35,194,221,123,217,148, 18, 27, 87,163,
95,131,101,160,201,249, 20, 15, 43,129,190,224,106, 93, 86, 39,
38, 45,172,178, 25,149,130,242,254,195, 31,166,251, 98,180, 50,
134,179, 13,147,222, 73,216, 8,231,125, 22,228,241,187,188,150,
213,244, 6, 51, 61,255, 29, 4,137, 68, 53, 91,232,196,145, 66,
44, 71,200,252,103,212,227, 49, 99,215, 70,218,243,164,181, 88,
79,198, 36,112,171,210,124, 57, 69,120, 74, 60,235,204,151, 7,
33,132,121,161,175, 72, 96,118,140, 41, 28,223,117, 47,142, 76,
55,107,155,192, 14,122,111,156,167, 30, 62, 12,144,162,126,114,
237, 32, 48, 97,207,219, 17, 34,197,138,182, 77, 19,245, 81, 64,

5,240,250,116, 16,157,173,229,208,109,110,127, 9,105,100, 37,
 170, 46,236,169, 58,226,176, 3,220,206,248,136,214, 89,158, 2,
 113,154,247,146,199,135,165,191, 83, 84, 75,104, 92,209,153, 67,
 239,202, 23,115, 24,141,186,185, 65,189, 0,108,133, 80,234,205,
 193,225, 52, 21, 78,253,184, 42,238, 10,183, 82, 26,168,152, 40,
 183,211,114,100,167, 46, 57,174,225, 79,162,229,234,139,230, 65,
 127, 24, 68,160, 45,171,213,151,109, 38,236, 34,250,153,226,161,
 134, 98,156, 76,245, 35,173, 56, 77, 11, 9,117,136,217,193,105,
 33, 5,140,198,222,200, 1, 10,224,178, 82, 41, 90, 80, 29,179,
 23,144, 4, 91,129,142,181,155,204,132,149, 53,201,163,192, 74,
 247,108,146,235, 36, 72,116,231,119, 62,154,206,209,159,176,221,
 248, 47,242, 84,169, 52,187,125, 13,110,107,141,218, 27,115,165,
 238,223,128,158, 54,112, 7,126,137,118,101, 32, 86,170,180,220,
 25,150, 12,186, 73, 19, 0,122, 94,157, 83,143,251,106, 21, 89,
 61,131,210, 67,195, 39,111,147, 92,172,124,228, 20, 66,253, 81,
 190,177, 87,130,232, 44,239, 97,133, 3, 26, 17, 16,188,203, 31,
 75,168, 58, 48,249,104, 22,191,120,215, 63,121, 60, 37, 69, 18,
 88,138,241, 78,184,233,103, 64,207,185,227,194,202, 96, 70,216,
 152,254, 49, 95,255,219,175, 8,196,145,252,199,123, 30,243,237,
 212, 93,214, 28, 55, 71, 99, 51, 59, 2,189,164,182,166,102,197,
 42, 15, 40,244, 6,208, 50, 43, 85,240,135,246, 14,113,148,205,
 26, 90,130, 27,222,247,102, 78,109,168, 11, 64,251, 9,120, 81,
 7,240,193,219, 53,236, 62,117, 29,172,115,213,163,204,177,211,
 170,162,131, 67,205,134,253,191,189, 80,137, 95, 8,238, 76,146,
 160,140,209,210,133,169,255,121, 42,239,123,125,157,138, 25, 46,
 181, 24,228, 92, 74,127, 89, 84, 68,173,111,199,185, 85,155,237,
 3,156,175, 98,149, 35,216, 38, 66,248,165, 65, 18, 32,142, 0,
 182,116,221, 16,112,252, 36, 73, 4,122, 99,176,154,100, 88,200,
 110, 54, 71,171, 96,126,226, 12, 72,202,180,174, 97,242, 51, 39,
 108, 83, 91, 93,118, 41,179,235, 10,164,245, 23, 6,104,192,214,
 15, 77, 70,150, 21, 50,143, 19,101,145,151, 45,249, 59,234,147,
 55,139,194, 63,129,218, 47,229, 48,215, 58,201,217, 57, 61, 2,
 107,212, 44,208,105, 34,178,113,132, 37, 33, 87,190,220, 5,148,
 246,187,225,230, 22,166,136, 82,152,233, 60,244,128,231,103, 94,
 52,203, 28,153,206, 30, 13, 49,183, 86, 17, 20,141,159,207, 1,
 188, 79,119,114,161,158, 56, 31,198,224, 14,186, 43,135,144,106,
 197,195,167,196, 40,232,184,241, 69,227, 75,124,243,223,250,254,

S[2]

88, 11,224,181,201, 79,173,194, 96, 47,129, 39,123,161,110, 32,
41, 19, 34,130,217, 71,220,116,233,147,178, 63,237, 57, 64, 73,
90, 85,191, 56, 60, 66, 50, 95,102,148,223,128,177,125, 7, 61,
165,212, 46,240, 58, 84,151,179, 29,127,131,105, 75,140, 1, 45,
98,171,163,229,207, 4,132,210,230, 0, 10,246,234,103,247,184,
111,101,175, 22,118, 14, 17,250,185,109, 12,160,121,155,238, 81,
176, 6, 77,180, 78, 31,138,170,157, 2,164, 23, 54, 35, 92,192,
62, 67, 33, 52, 44,134,198, 13,115,215,156,235,206,190,141, 80,
152, 99,133, 93,213, 97,214, 3,114,254,139,204,253, 72,248,251,
226, 89, 53,124,245,199,225, 68,197,166,162,135, 21, 87, 36,202,
30,243,188, 70, 94,100,117,137,126, 49, 37,145,200, 86,112,159,
20, 65, 26,104,149,189,168,218,169,203, 8, 74,193, 28, 51,255,
219,174, 42,221,120, 48,158,227,108,208,182, 27,106, 18, 38, 15,
25,153,119,232,167,144,222,241,231, 91, 83, 40,113,196,143,211,
236, 76,228,150,205,195, 9,136, 24,242,186, 82,172, 5, 16, 43,
216,154,187,249,142,239,252,146, 55,122, 69,183,107,244, 59,209,
198,141, 18,216,230, 50, 8,231,149,204,243, 38,250,168, 48, 82,
151,220, 31,114,244, 83, 62, 90,131,171, 78,113,107,143,152,106,
140, 55,196,147, 29,119,236, 80, 51,209, 74,207,242,184,211,173,
255,169, 69,154,178, 71,117,150,134, 4,237, 12,137,157,111,162,
251,176,234,205,206,155,180,179, 67, 17, 43, 3, 19,227, 61, 22,
239,222, 1, 47, 58,182,232, 75,241,201,153,218, 72,199, 20,197,
32,126,214,233, 40, 2, 14,208,175,159,142, 36,144,128,192, 7,
93,225, 70, 63,186,120, 73,215,174, 99,123,188,224, 84, 97,160,
240,112, 21,132, 64, 89,121,130, 91,135, 10, 15,148, 92, 42, 5,
191, 81, 76, 41,125,226,101, 11,170, 87, 0,185,202, 65, 34,183,
109,248,229, 13, 23,166,219,247, 95,139,217,105,129,238,103, 24,
116,163, 33,212,235,189,172,122, 49, 9,194, 54,181,177,252, 6,
254, 27, 30, 60,108, 39, 53,145,138,213,190, 16,167, 56,246, 94,
35, 86, 28,156, 52, 68,221,124, 57,110,210,133, 77, 45,158, 85,
100, 88, 44,245, 98, 79,102, 59,104,187,249,127,195,118, 96,146,
37,200,253, 66,228, 26,115,223,165,161, 25, 46,136,164,193,203,
160,197, 1,186, 44,116,183,153, 75,254,144,246,239, 11, 0,170,
76,175,117, 57,189, 40, 29, 73,219, 93, 4,248,150, 81, 56, 96,
182,156, 82,162,126,231,242, 83,196, 24,119, 69,226,255,206,178,
167, 12,105,168,155,109, 49, 7,122, 78, 32,118,204, 33,157,218,
190,138,211,111,115,108,251,128, 28,209,241, 26,240, 67,230,235,
141,120,131, 64, 17, 6, 77,158,221, 79,130, 58,187, 39,121, 48,
202,188,143, 19,223, 46,220,140, 86, 65, 16,154,215,164,253,185,
181, 60,210,243, 30, 85,198,102, 90,169,208,224, 45,193,133, 55,
145, 63,203, 50, 61, 51,177,149, 5, 92,233, 68, 95, 71, 91, 9,
129, 59,132, 3,236,194,114,110,104,229, 53,199, 97,222,214,216,
146, 84,134, 98,173,234, 99, 42, 52,100,200,195,201,165,232, 2,
35, 20, 27,252,103,245,227,123,101,137, 13,107, 41,161, 43, 23,
14, 66,171,249,250,112, 18,163, 10,213,127,217, 88, 87, 94,212,

124,172,180,238,113,179, 15, 74,135, 47,142,147,151, 25, 8,148,
36,225, 37, 89,184,174,136, 54,139,228,159,125,247,244,106, 34,
191, 72,205,237, 38,152, 80, 62,207, 21, 70,176, 31,192,166, 22,
239,166, 81, 97,179,148,207,225,129,119,130,205,193,131, 33, 70,
42, 2,245,187,146, 7, 77,231, 6,147,143,107,227, 47, 63,216,
115, 88, 95, 24, 69,133,254,243,233, 57,102, 40, 39,155, 18,171,
41,144,125,117, 99, 48,210,108,251,151,158,110,113, 27, 13,114,
19,209,212,242,136,116, 38,149, 84, 90,192,168,152, 53, 14, 75,
72, 85,186, 16,167, 87, 15,220, 64, 5, 22,154,138,228, 3, 35,
162, 10,248, 79, 9,120, 37,105,232,169, 26,177, 55,122,196, 94,
153,180,188, 49,201,255, 36,163, 82,106,128, 80,250,189,104, 25,
181, 68, 32, 51, 67, 62,103, 29,134,234,126,174, 50,197,195, 45,
238,176, 0, 96, 76, 12,224, 1,100, 28,184,199,241,145,118, 61,
101, 78, 46,217,230,140, 56,194,183,252,173,127, 91,200, 17, 65,
190,161,157, 54,211,137,247, 71,150, 89,124,132, 20,121,222, 23,
253,172,191, 43, 74,159,240,165,198,237,235, 83, 92,203, 58, 59,
98,156,112, 30,170, 4,139,160,164,213, 21,206,236,111,229,208,
86,123,202,226,246, 52,218,219, 31, 66,178,141,204,221,142,223,
249, 73, 60, 34, 93,215, 8,175, 11,135,182,185,214,109, 44,244,
151,255,181,202,148,180,203, 47, 28,175,247, 57, 36,224, 77,232,
75,209, 69,183, 7,174, 43,186,167,195, 22, 53, 33,213,116,117,
80, 91, 82,179, 5,198,163, 32,105, 81, 12,184,234,154, 76,120,
149, 39,222,137,178,182, 95, 79,133,129, 68,141, 37,229, 89,132,
112, 88,191,220, 54, 51, 15,177,194,231,171,100,211, 23,214,217,
173,123,187,126,227,128,158,164, 48, 11,188, 4, 71,161,157, 78,
63,245, 73, 25,168,104,162,107,131,246,199,160,250,244,155,218,
10,172,206,240, 14,156,119, 52, 31,146,106,204, 8, 85,144,248,
254,205,166, 9,225,111, 19,101, 99, 46,150,110, 27,185,143,241,
201,235, 62, 3,139, 83,197, 90, 94,200,127,121,212,176,136, 42,
124,236, 34, 30, 38, 26, 16, 61, 74,118, 1,125, 64,109,239, 59,
98,138, 18,196, 21,190,165,134,113, 0,242, 65,252,152,249,207,
84,142, 60,122, 50,169, 87,208,108,230,115,210, 24,223, 66, 40,
159,114,193, 93,216,237,253, 41, 58,233, 35,130,221,145, 6,215,
135,238, 49,147,102, 2,226, 45,192, 55, 92,170, 72, 13,153,243,
96,251, 20,228, 29, 86, 44,219,140, 56, 70, 17, 67, 97,103,189,
234,233, 17, 89,238, 14, 93,194, 41,200,161,219,203, 90,104,166,
214, 45,173,150, 23,167, 61,179, 67, 79,211,103, 46, 70,146, 0,
2,154,208,112,187, 49,218,163, 84, 85,242,118,182,138, 83,212,
59,128, 58,207,149,170,247, 38,250, 24,216, 56, 3,204, 74,165,
228,113,110, 22,196,178,141,180,160,243,232,123,148, 71,225,239,
168,129,254, 33, 32,215,152,133,108, 68,127,183, 8, 64,114, 72,
19,120, 63, 65, 69, 87,224, 82,116,217,162, 5,237,115, 78,117,
11,107,185,157,174, 1, 29,198, 42,199,255, 95,177,190, 48,213,
197, 7,175,143,145,153,102, 57,176,142, 21,235, 44,231,202,132,
195, 55, 75, 98,240, 62, 16, 35,246,223,248, 88,205,230,253, 73,
171,188,193,140, 51,130,155,134,184,192, 99, 15, 27,131, 54,244,

53, 30, 13,220,151, 43, 36, 86,137, 18,227,159,105, 37,158,169,
81, 96,135,136,226, 52, 25, 28,210, 50,124, 31,106, 92, 12,100,
201, 97,111,144, 4,109, 6, 47, 40, 94, 76,252,126,164,249, 80,
10,229,236,241,139, 9,189,101,209, 26,245,251,156,206, 20, 34,
60,191,172,222,125,119, 66,181, 77,221,147, 39,121, 91,122,186,
248, 10, 13,147,188,180,105,104,245,165, 86,100, 37, 38,152, 24,
97,133, 81,218, 79,120,226,177, 30,220,150,194, 4, 47,215,243,
189,125, 93,173,212,159, 21,197, 87, 95, 52, 60, 65, 98, 69,121,
88,240, 58,172, 29,202, 66, 80,198, 25,183, 89,151, 36,169,252,
149,119, 71, 85, 68, 76, 8,108,207, 42, 2, 54, 34,219,164, 91,
158,138, 73, 44, 45, 16,250,192,103, 70,122, 6,167, 84,204,237,
5,163, 56,246,161,247, 19,124, 59,213, 0, 33,209,187,107,227,
175, 3,191,249,139,127,210,123,155,205, 31,224, 35, 18,153,222,
94,168,126, 51, 72,216,241, 64, 27,109, 53,135, 63, 39,190,113,
230, 17, 61,201,154,244,239,117, 92,179,196, 22,101, 15, 20,116,
41,156,144,176,142,136,106,223, 62, 12, 90,137, 99,131, 40, 96,
236,211,186,238, 78,208,141,255, 55,160,251, 26,174, 9,221, 67,
225,118,112,114, 77,195,233,110,235,203,170,134,184,242, 50, 57,
206,200,182,231, 82,193,130, 46, 7,162, 75,146,129,145,140,253,
11,102, 83,228,254, 49,171,143,199, 48, 1,234,157,232,229,111,
14,181, 32,185, 74, 23,166,178,148,115,214, 28, 43,217,132,128,
255, 67, 48,214, 93, 28,161,201,183, 94, 73,215, 33, 59,228, 12,
167,205,113, 15, 11,206,202,220, 16, 69,117,150, 41, 10,223, 39,
20,125,173, 29,139,112,243,178,102,210,142,248,249,213,209,122,
187, 1,182, 5,148,227, 52,194,144,245,254,107,219, 51,123,222,
90,236, 27, 72,162,137, 62,174, 9,145, 24,127,126,146,191, 37,
23,115, 89,141, 30,185,212,106,119, 65, 0,124, 66, 18,224,198,
128, 97,239,156,207,136,105,235, 81,116,138, 35, 78,177, 34,241,
169,225, 21,242, 91, 49, 7,186,109, 13, 58,132, 61,129,175,110,
101,104, 50,108,179, 22,130, 45,103, 99,120,152,157,240,140,131,
42, 56,229,135, 46,234,192,121, 57, 44,147,244,170, 55, 31,233,
154,143,149, 2,226,211,189, 82, 92, 74,151, 87,218, 86,133,197,
247,195, 25, 26,208, 38,172,176, 8,251,188,111,164,221, 75,200,
166,238,171,203, 43, 79, 83, 6, 71,253,237,230,184,118,232, 40,
193, 95,158, 80,190, 14,159, 68, 84, 19,160, 63, 54, 76,153, 85,
77, 53, 32,246, 96,168,199,114,180, 88, 17,134, 98, 70, 60,217,
252, 47,231,181, 36,165, 4, 3,204,216,100,155, 64,196,250,163,

S[3]

250,158, 23, 8,253, 67,238, 34,179, 56,166,152, 60, 48, 37, 74,
211,217,202, 25, 4,184,210, 53,224, 96,164,254,231,220, 75,181,
146, 21,101, 7,150, 43, 22,175, 98, 11,156,218,222,189,212,100,
112, 61,251, 71, 17, 54, 40,229, 87, 58,195, 2,237,208,239,244,
134, 72, 94,137,162,127,121,191,194, 38, 85, 15, 47, 88, 83,114,
63,225, 30,139,173,123,141, 49, 41,118, 81, 39,241,206,106, 50,
163,172,198,111, 9,182,209,186,216,192,105,235,252,160, 68, 28,
168, 31,124, 51,227,221,153,132,170, 62,197,125,140,116,248, 79,
77,185,104,169,180,155, 27,113,171,174,154, 36,119,107,187,188,
165, 10, 97, 24, 59,157, 73, 0, 78, 66, 3,215, 5,148, 1, 52,
13, 57,226, 90,103,136,177,249,102,196, 89, 95, 32, 19,245,223,
120,228, 46,232, 35,131, 16, 44, 20,214,135,247,126,161,213,255,
42,243, 65, 6, 82,183,110, 92,233, 12,147,108,129, 91,219,207,
99,138, 93,203,144,109,178,145,143,176,242,201,236,190, 55,205,
199,204,200, 80, 14, 64, 33,246,193, 76,133, 70,167,128,240, 29,
117,234,230,151,142, 45,159,115, 18, 26, 69,130, 86,149, 84,122,
199,151,211, 86,105,248,178,220, 95,171, 68,195,174, 29,197, 21,
28, 17, 66,170,225,244, 60, 62,172,155,167,210,161,190, 14, 30,
27, 43, 32, 38, 79, 39, 5,134,117,166,125, 55,214, 2,196, 78,
44,164,114,173, 94, 25,194,157,200, 37,252,221,222, 7,251, 10,
150,160, 85,159, 54,198,243,146, 67,230, 31,184,141, 40, 71,130,
63,103,203,118,154,101,110,121, 13,102, 93, 89,232,153,216,236,
50, 65, 26, 16, 58, 57,185,183,156,235,187, 64, 11,231, 59,119,
70,223,128,188,131, 88,165, 76,193, 96,107,189,209,149,238,192,
246, 42, 75,175,234, 80, 48, 35, 72, 23,204,247,250, 19,233,162,
217,147, 46, 45, 36, 99,177,126,129, 61, 3, 49,158, 47,163,152,
53,136,239,224,180,148,127,176,255,109, 0, 33, 97,212,138,104,
228,142,112,179, 51,254,218,111,143,120,205, 69,108,206,135,186,
113,144,122,215,133,168,115,123,253,137,201, 90,202,169,182,213,
77,181,237, 8,132,124, 41, 83, 82, 81, 74,245, 20,116,227, 92,
18,191, 9,145,242, 87, 6, 4,106,208, 22, 24,139,100,229, 84,
249,226,241,207, 98,219, 15,240, 12, 34, 91, 56,140, 1, 73, 52,
139,109,214,232,203, 65,112,205,192, 10, 23, 75, 82,234,208, 18,
128,117, 37,115,223,147,217, 33,201,150, 73, 0,211,156,163,118,
93,200,172,165,182, 19, 27,246, 40, 15,184, 29,227,241,180, 95,
24,124,125,226,251, 59, 11, 83,222,111,126,158, 66,116, 43, 67,
9,134,245, 88, 70, 98,206,114,171,120, 62,127, 3,132,152,244,
69, 54,104,210, 79, 94,153, 63,102,252, 84,105, 61, 30,231, 22,
103, 57,236,161, 71,141, 41,218, 50,169, 46, 49, 34,133, 81,187,
177,196,202, 20, 35,190,220, 26, 48,194,209,185,155,136, 21,151,
8, 89, 96,162,174, 13,181, 58, 4,121, 31, 78,157, 2,216, 91,
32,119, 56, 36,186,178, 5,173, 99,247, 90, 92,146,131,167,207,
253,122,183,237,225, 16,199,137, 39,233,239, 52, 38,240,110,176,
123, 76,255,242,254,250,164, 97, 77,179,243, 17,138, 72, 45,197,
195,143,228,191,154,198, 64, 44,229,135,113,106, 85,224, 28, 1,

100,193,129,142,212, 68,249,175,166,189,235,221,159, 7,144,108,
42,148,215, 87, 74,213,230,248,170,168,140, 86,219,145, 51,130,
25, 14,107, 55,204,101, 47,238,160, 53,149,188, 6, 60, 80, 12,
251,247,201,134,182,179, 83,118,123,160,149,230,243,213, 79,166,
190,138, 28, 71, 61, 93,154,238,232,205,162,133, 35,128,223, 19,
45,184, 12, 44, 46, 62,226, 5, 47,245,177,102, 23,129,101, 22,
199,100,136,254,207,196, 24, 32,135, 17,253,220,147, 8,202,249,
39, 30, 88, 2, 58,244,211,173,124,216,250,122, 55,181,127,146,
180,248,117,235,137,116, 98,107, 6, 96,210,106,214,142,237,231,
172,175, 1,215,131,183, 57,152,217, 40, 11, 42,200, 33, 80, 82,
18,209,178,113,174, 54,161, 60,203,241,130,221, 78,169,188,119,
168,148,225,115,204,139,163,228,165,176,110,170,224,186, 76,227,
239, 99,143,132, 15,150, 85, 72, 74, 73,212,198, 91, 51, 10,158,
233,195,126, 49, 84,193, 56, 65,167,156, 90,242,153, 21, 66, 38,
252,144, 9, 63, 97,112, 52,155, 77, 25, 41, 69, 20, 27,222, 92,
255,121,159,114,208, 67,171,185,105, 53, 70,194,206,192,109,229,
187,104,103,151, 7,246,189,125, 87, 34, 59, 0, 3, 4,218, 14,
94,111, 29, 50, 89,191,141,234, 37, 43,120,219, 68,157, 64,240,
86,236,140, 26, 95,108, 13,164,145,197, 48, 16, 36, 75, 31, 81,
218, 58,139,114, 54,212, 45,207,174, 1,197,148,135,155,227,104,
88,187, 75, 90,225,237,111, 89, 52,211,204,165,170, 55, 28,129,
78,151,143,232, 98,153,136, 60,141,209,161,119,158,217,137,229,
59,109, 74,222, 99,138, 16, 50, 32,115, 5,168,185,205,221, 86,
21,100,252, 67, 34,235, 14,247,178,156,173, 2, 0,133,172,108,
214,231,249,160,181, 22, 11,189, 94,200,126, 9, 49,132,154,149,
157,167,162, 20, 35,213, 44,196, 18, 61, 70,118,230,194, 42,255,
243,215, 73,244,127,159,145,233, 33,236,201, 39,113, 71,246, 13,
131,239, 63,150, 65, 6,190,128,117, 93,179, 85,195, 47,199, 96,
193,144,152, 25,203,124,166,103,175, 97,125, 23,202, 92,250, 36,
242, 66,251, 24, 79,140, 53,245,210,224,219,191, 29,186,147,164,
8,106,238,120,102,121,163,248,169, 7, 84, 10, 31,253, 83, 43,
82,101,206,220, 72,254, 48, 3, 68, 37,188,171,130, 81,105, 46,
134, 57, 12,241, 15,216, 27,240,228,183,122,223,110,198, 87,107,
4,177,208, 38, 77,234,180, 76, 62,123,112,184, 19,142,192, 56,
41, 40,146,176,226, 95, 91, 26, 51, 30, 64,182,116, 17, 80, 69,
115, 77, 82,199, 99,207, 43,149,196,105,214,163,108, 6,201,134,
252,246, 60,143,211,123,164,222, 62,165, 49,203,219, 20, 36, 80,
208,197, 22, 50,226,227,202,238, 48,144, 10,247,159, 52,215,200,
169,138,146, 84,139,170,225,237, 18, 83,232, 76,113,156, 2,148,
1,106, 78,251,136, 81,161,125,135,122,212,176,173,186,121, 3,
97, 23,118,120,167,180,217,129, 44,100,243,242,128,231, 70, 69,
19,102,133, 40, 57,158, 67,189, 74,107,213, 56,142,210, 75, 95,
249,116,187, 53, 46, 65,248,236,230, 11,119, 87,193, 45,209, 32,
47, 63, 4,145, 30, 94, 96,228, 8, 88,114,198, 64, 14, 54,112,
17,204, 37,223, 66,166,178,124,151,157,216, 26, 68,175,191, 33,
185, 13, 86, 31,103, 98,147,132,181,101,160, 24,239,244,190, 72,

42, 59, 92, 255, 254, 150, 194, 61, 104, 220, 179, 171, 58, 183, 131, 182,
110, 12, 224, 184, 79, 188, 206, 109, 250, 126, 90, 35, 93, 205, 229, 195,
140, 73, 39, 25, 234, 27, 15, 155, 233, 21, 7, 192, 41, 240, 29, 111,
16, 172, 34, 137, 55, 71, 154, 130, 153, 91, 141, 127, 174, 245, 38, 5,
51, 177, 89, 241, 168, 218, 235, 253, 152, 9, 85, 28, 0, 221, 162, 117,
230, 62, 228, 1, 0, 55, 138, 149, 202, 242, 223, 41, 96, 184, 131, 144,
27, 188, 68, 86, 173, 31, 91, 2, 169, 98, 171, 255, 224, 106, 140, 22,
28, 56, 239, 20, 105, 116, 236, 215, 164, 205, 11, 6, 78, 43, 93, 178,
107, 174, 247, 129, 45, 101, 80, 146, 122, 89, 200, 207, 214, 53, 217, 132,
135, 121, 113, 74, 70, 83, 244, 58, 151, 196, 232, 108, 25, 104, 7, 210,
128, 201, 250, 190, 153, 204, 130, 84, 110, 159, 18, 226, 30, 170, 61, 211,
38, 47, 37, 109, 9, 145, 253, 48, 51, 88, 199, 189, 183, 95, 234, 218,
64, 32, 123, 172, 92, 168, 147, 220, 97, 65, 198, 180, 72, 182, 134, 156,
231, 35, 175, 103, 57, 75, 17, 216, 10, 213, 23, 114, 158, 29, 245, 237,
39, 243, 19, 59, 152, 77, 206, 148, 33, 87, 112, 8, 50, 13, 212, 60,
90, 143, 79, 233, 179, 115, 34, 161, 124, 15, 157, 36, 133, 21, 221, 241,
193, 5, 44, 49, 181, 141, 118, 76, 208, 246, 197, 177, 46, 227, 167, 67,
195, 54, 100, 187, 222, 117, 94, 4, 139, 102, 248, 85, 254, 203, 99, 42,
235, 14, 26, 194, 176, 82, 163, 12, 209, 186, 69, 73, 3, 155, 162, 40,
111, 251, 63, 154, 219, 52, 137, 240, 71, 229, 238, 165, 126, 150, 66, 142,
252, 185, 127, 249, 125, 16, 191, 225, 81, 166, 24, 136, 192, 119, 160, 120,
46, 8, 0, 32, 57, 123, 52, 10, 132, 20, 249, 60, 211, 92, 97, 99,
7, 6, 118, 201, 131, 128, 43, 134, 151, 25, 190, 51, 105, 104, 30, 95,
228, 173, 3, 73, 231, 195, 108, 27, 200, 184, 244, 58, 177, 82, 28, 81,
158, 12, 2, 138, 64, 145, 117, 250, 84, 143, 161, 62, 85, 168, 72, 69,
68, 77, 241, 203, 160, 39, 180, 38, 147, 70, 79, 166, 124, 18, 154, 142,
209, 153, 50, 23, 75, 112, 33, 206, 103, 106, 189, 169, 101, 78, 233, 245,
54, 174, 176, 35, 93, 234, 15, 114, 227, 63, 9, 1, 91, 159, 223, 96,
110, 237, 149, 116, 87, 205, 202, 204, 83, 94, 187, 86, 16, 125, 144, 220,
113, 102, 122, 14, 196, 238, 181, 235, 226, 192, 109, 76, 146, 100, 111, 191,
230, 98, 129, 251, 163, 56, 224, 65, 253, 133, 34, 31, 208, 74, 45, 185,
254, 13, 135, 88, 219, 140, 44, 47, 213, 170, 183, 247, 252, 248, 90, 11,
212, 29, 215, 182, 22, 194, 214, 210, 240, 24, 141, 239, 162, 80, 172, 136,
21, 218, 130, 36, 165, 167, 66, 179, 19, 178, 61, 175, 236, 67, 155, 59,
4, 225, 207, 89, 148, 157, 17, 221, 121, 171, 49, 115, 199, 150, 188, 55,
107, 246, 217, 127, 255, 197, 232, 5, 242, 139, 119, 186, 42, 40, 137, 198,
156, 243, 41, 120, 193, 164, 48, 152, 216, 26, 37, 71, 126, 53, 222, 229,

S[4]

246,144,239,106,173, 98, 46,166,211,104,249, 26, 64,130, 84,138,
 154, 19, 12,133, 61, 13,161,157, 49,192,224, 25,112,232, 81, 93,
 134,155,160, 71, 52,205,188, 65,153,100,172,194, 73, 95, 36,110,
 216, 79,125, 21,174, 75, 53,159,222,165, 83, 7,209,178, 48,187,
 176, 17,230, 9, 37, 66,191,225,197, 23,244, 27, 86,169,179, 3,
 34,220,202, 62,143,248,183, 44,237,103,227,116, 6,126,251,240,
 193,212, 35, 60,149,145, 76,254, 40,242, 30,171,140,217, 77,218,
 213,235, 5,185,141,127,102,253,163, 54,189, 55,236,210,231, 80,
 107, 1,105,233,250, 85,114, 58,128,119, 87,122, 33,195,245,241,
 203,243,190, 92,150,123,208, 11,111,121, 88, 59, 78,226,146,206,
 43,207, 91, 38,196,170, 0,201,108,200,168, 18,221, 32, 96,255,
 113,129, 69, 68, 41,117, 90,115, 63,204,156,109,124, 57, 29, 56,
 99, 94,118, 20,136,177,135,219, 10,223, 82, 31,199,252, 42,162,
 148,186, 70,164,167, 89,182,234,215, 72, 16, 15,142,152, 51, 39,
 131,238, 47,228, 28, 67,247, 74, 2,180, 14, 24,229, 45,184,132,
 4,139,101,137, 97,158,147,120, 50,181,151, 8,175,214, 22,198,
 14,124, 40, 6, 13,166,197,123, 30, 42,213,191, 23,195,232,253,
 35,106, 51, 86,189, 28, 26,117,101,244,174, 52,217,126,109, 99,
 203,141, 3, 94,225,245,145,132, 50,159,136,239,243, 29, 65,205,
 206, 92, 25,113,120,214, 38,153,147,247,224,138,223,215,252,111,
 140, 70,154,171, 22, 83,233,199,229,194, 73, 43,149, 44, 58,193,
 39,116,112,130, 15,148,204,178,100,142,158, 34,129,181, 96, 91,
 222, 72, 7, 4,190,237, 33, 5,107,240, 64,235, 1,162, 95, 57,
 175,108,103, 79,182, 69,135,110,176, 21,234,172, 27, 67,221,118,
 24, 36, 75, 76, 20,183,125,248,114,168,220, 17, 78,230,115,155,
 201,134, 48, 56,202, 87, 19, 98,251,131,165, 16,170,209,242, 62,
 139,151, 9, 71,218,169,144,152,143, 46, 77,246,177,121,219, 37,
 32,192,105,198,133,187, 84, 45, 93,128,249,102, 11, 60, 8, 68,
 104, 49, 88,236,150, 66,212,180,210,127,231,119,228,241,200, 89,
 80, 31, 2,122, 12,216, 63, 97, 53, 18,146, 61,188,157,196,207,
 208,161, 54,156, 81,255, 82, 47,167, 55,163,164, 90,173,179, 74,
 85,186,250, 41,185,160,226, 0,238,227,184,137,254, 59,211, 10,
 193,188,153,200,109, 99,230, 21, 15, 63,133, 94,126, 92, 69,112,
 91, 79,154,141, 26,139,116, 51,228,250, 57,107,138,171,205, 59,
 24, 70, 77,199, 54,191, 22,160,173, 83,158, 42,122,185,233, 38,
 62, 84,214,248,254, 68, 40,177,212,135,150, 16, 17, 53,157,206,
 67,170,252, 34,220, 12,245, 9,129,131, 44, 75,176,156, 55, 14,
 103,134, 3,232, 52, 27,243, 71, 25,100,238,215,114, 36, 46, 50,
 61,104,161,249,106,102,142,219,234,229, 4, 48,101, 23, 37,169,
 64, 43,198,189,137, 86, 98, 33,213, 0,105, 10, 2,210,217, 32,
 239, 8,231,183, 20, 60,159,120,149, 7,216,196,165,246, 58, 80,
 146,227,235,117, 89, 19,140,174,181,127,221,121,128, 87,111,152,
 166,190,130,218,223, 49, 90,124,164,237,113,175,241,204, 65,247,
 207,225,195,148,125, 6, 5,119, 76, 28, 85, 30,151,172,203,168,
 244, 18, 1,208, 95, 35,201,192, 97,255,253, 96,182, 78, 39, 72,

118, 31,187,194, 56,167,123,144,184,251,180,240, 82,155,226,147,
73,162,108,211, 41,186, 81,132, 47, 11,236,136,179, 66,222,110,
29, 93,145,209, 88,224,202, 74, 13,115,143,242,163, 45,197,178,
173,251, 22, 23, 32,145,153,219, 55, 0,221,210, 72, 8,103, 4,
38,193,127, 88,222,216, 10, 95,141,151,104,203, 96,231,106,209,
229, 39, 58,206,232,167, 6, 2,177,247, 25, 94,225, 65,101,202,
199, 80,147, 40,208, 45, 92, 86, 36,237,175, 66, 11, 78,144,149,
119, 17, 52,197, 51,172,143,249,113, 50, 54,150, 81,243,126,124,
186,161, 57,244,156,254, 20,191,187,185, 29,122, 44,140,163, 15,
158, 31, 27, 83,109,148,227,228, 49, 9, 3,214,171, 75, 1, 90,
162, 85,245, 71, 47,146,189, 13, 59,205,159, 84, 24,128,123,155,
194,115,246,142, 91,201, 43,116, 87, 89,170,133,168,154,160,207,
134, 5,255,131, 53,248,137,132,117, 60, 77, 93, 16,184,195,234,
110,200,242,108, 56,179, 26,181,188,239, 7,114, 33,233,178,102,
64,240,220,118,164, 63,224, 67,138,139,182,166,183,100,241, 73,
105,130,218,236, 41, 79, 99, 18,107,212, 76,223, 68,204,121,136,
252,157, 35,211,169,125,129,230,192,190, 28,226,152, 30,253, 48,
238, 34, 97, 69,165, 21, 46,120, 82,135,111, 61,196, 14, 37,250,
98,217,174,112,213,215,198, 19, 12, 42,235, 70,176, 74, 62,180,
204,237,105, 94, 22,142,203, 53,141,233, 58,187,218, 31,223,122,
120,130, 9, 42, 72,212,201,192,173,238,251,216, 63,198,243,134,
79,227,235, 99,131,179, 41,169, 57, 64, 87, 15,110,255,157,107,
70, 66,232, 38, 29,136,135,119,195,140, 17, 67,241,137,188,127,
222,102,146,153,239, 89, 45,159, 71,230,245, 36,103,226, 32,244,
214,197,206,106,182, 93,139, 60,170, 92,190,189, 73,250, 48,176,
95,246,234, 86,111, 47, 39, 52, 77,247, 1,199, 10,186,221,209,
129,213, 44,178,101,224, 8, 23,196, 14,155, 4,154,208,166,207,
253,126, 78, 84, 61,145,162,151,205, 7, 88, 51,172,163, 55,174,
35,236,252, 62,211,149,229,100, 34, 6,123, 76, 25,193,147,171,
16, 69, 97, 13,231,185,228,219, 33,164, 83,167, 56, 82, 12,112,
184, 20, 59,121,125, 96,109, 81,249, 49, 21,161,115,242,254, 3,
152,210, 2, 50, 30,117,138,240, 80,225,168, 18, 75, 65,144, 28,
98,248,202,124,220, 91,217, 46,200,108, 11, 68,128, 26,104,181,
116, 74, 0,191, 5,118,148, 85,150, 24,133, 40, 27, 54,177,194,
143,158, 19,132,180,114,113,183,165, 43,215, 37,156, 90,160,175,
82, 63, 95,202,190,224,131,140, 99, 48,154, 2,139,243, 70,135,
21, 73,127,160,188,222,239,252, 93,142,111, 15,215, 29,159,219,
65,107,156,220,234,136, 76, 77, 50,123,162, 90,246, 98,175, 1,
104, 6,194,125,112,169, 91,184,209,153,101, 58,228, 45,226,223,
12, 38, 30,221,119,116, 7, 44, 54,115, 72,189,255, 28,144,214,
102, 36,146,241, 87, 8, 85,207,247, 11, 35,192,196,105,245, 9,
42,183,213,166,147,232,200, 74, 92,150,201, 61,251, 43,198, 83,
94, 22,187,235, 27, 79,122,199,158,130, 14, 89, 52, 0, 68,172,
133,143, 66,167, 62, 67, 56, 31,170,237,141,120,240, 18,216,176,
121, 57,208, 51,182, 10, 96,225,248,236,173,186,117, 26, 59,180,
205, 71,118,163, 40,171,193, 55, 81,106, 80,253, 53, 69,103, 13,

244,126,195, 49, 20,191, 39,148,179,227, 33,165,134,233, 3,206,
137,155, 19, 84,152,149,181,229,204,203,249, 78,157,113, 32,108,
168,210,110,161, 46,129, 4,124,217,218,250,211, 75, 34, 41, 97,
145,212,114, 5,128,231,132,109,197,242, 24,100,164, 16,138, 88,
25, 86, 37,185, 47,178,230, 60,174, 17,238,177, 23,254,151, 64,
47, 24,122,254,137, 82,116,214,107,138, 48,184,221, 84,108,131,
191,142,139,144,130,120,229,117,140,115,208, 56,175,152, 34,149,
242, 46, 94,218, 36, 65,109,198,204, 31, 77,161, 76, 58, 63, 81,
86,193, 1,141, 83, 73, 70,156,166,162,185,199, 78,192,196,224,
255,182,136, 38, 12,250,253, 88,178, 92,247,251, 23,105,150, 6,
79, 25,207,126,148, 52,197,231, 60, 7, 10,128,104, 44,165, 16,
249, 35, 80,110, 50, 5, 33, 59, 39,168, 45,153, 40, 49, 4,155,
103,235, 93,101, 91, 37, 41,170, 14,188, 22,223, 11,119,158, 87,
8,100, 69,180,232, 90,211,177, 55,145,159,194,164,133,172,252,
219,183,238,244,106,123,113,200, 17, 51, 13,163,173,209, 19,239,
3, 89,240,233, 20,171, 32,167, 99,210, 72,237, 30, 68,134,187,
28,213,215,206,234,225,241, 57,169, 2, 98, 15, 71,236, 27,135,
127,205,201,216,246, 29,248,186,203, 61, 64,227,212,179, 26,189,
217, 9, 75,181,129, 95, 97,154,111, 96,151,143, 54,190,121,228,
202,222,160, 0, 62, 66,146,125,245,243,174, 67,230, 21,118, 53,
102,132, 85,176,195,114,124,226, 18,112, 42, 43, 74,220,147,157,
250,118, 3,239,107, 51, 4, 59,117, 83, 68,105,169,176,209,189,
41, 58, 72,104,183,151,100,212,208,103,148,162, 20, 61,122, 88,
55,142,202, 80, 99,126, 60,216, 15,127, 14,222,179,140,138, 87,
78, 77, 11,146,229,166, 65, 40,131,214, 71,178,255,237, 10,247,
186,157, 13,120,135,243,111, 47,215,207,184,108,149, 84,231,167,
123,180, 1, 52,159, 23,165, 43,109,156,164,136,241,234,174, 36,
246, 74,196, 34,125, 48, 22,175, 6,235,200, 42, 37,145,168,101,
225,160,141,143,194,113,185,248,106,230,249,124, 86,224, 82,181,
24, 38, 97, 29, 7,199, 18,238,110,128, 91, 39, 67, 2,220, 9,
219, 56,155,217, 94,203,205, 63,188,195,137,153, 75,242,182,114,
198, 32,253, 16, 85, 33, 44,192, 0, 79,223, 35,134, 73,133,201,
221, 45,173,158,171, 31, 30,211,245,112,152,177,233,227, 57,197,
92, 64, 19,190,129, 26,163,150, 70,119, 69,132, 50,213, 93, 66,
8, 98, 12,218, 54, 25,170,191,204,115, 5,226, 49, 90,236, 17,
244, 28, 76,130,251, 62,161, 27,232, 81,121, 96,139, 95,147,210,
144,193,228,172,252,154,102,240, 46,206,187, 89,254, 53, 21,116,

S[5]

235, 51, 83,157,164,168,224,101, 22,175, 11, 80, 55,174, 44,125,
0, 70, 33,117,190, 23,187,102, 78, 99,182,192,177,141,216,249,
4, 92, 14,156,127, 15,233, 5,210,234,198,186,172,188,220, 93,
118,138, 68, 40, 66,222,251,143,202,146,176,140,167,227, 62,136,
124,244,119,108,163,116,152,134,197,109,183,129,229, 77,255, 26,
106,195,107, 37,230, 19,242,212, 46, 89,154,180,100,150,237, 54,
45,231,201,144,200,178,160,149, 59,103,115, 60, 58,165,252,104,
91, 67,114,110, 86,225, 95,215,218, 64,179,139, 72,113, 75,219,
73, 96, 20, 16,131,137,142, 29, 9,159, 25,133,173,184,246,132,
161,228, 90,122,213, 24,250,171, 13,203,181,169,135,207,151,194,
36, 84, 21, 81,111, 52,239, 42,112,196, 97,208, 56,153, 61,243,
241,232,206, 10, 38,236,209, 12, 53,170,199, 82, 87,248, 85,217,
17, 2, 65, 31, 47,123, 76, 79,105,166, 98,126, 35, 63,121, 28,
148,162, 7, 34, 71, 43, 30, 88,223,240,238,253, 18,193,211,189,
214, 6, 3, 74, 41,155, 48, 94,205, 57,147,221, 32, 50,204,185,
27,226,254,128,120, 1, 8, 49, 69,145,158, 39,191,245,247,130,
171, 67, 80, 7,233,145,252,141, 26,196, 32, 37, 77,150,136,236,
1,223,124,214,179,225,235,134, 57,195,177,132, 61, 81, 19, 93,
189,126,155,172,123,140, 8, 98,113, 48,128, 9,163, 14,149,178,
153,137, 21,125,131,162, 42,142,206, 17,143, 78,191,249,139,212,
111,158,106,176, 15,210, 0,217, 56,192, 64, 63,239, 88,135,238,
215, 10,121, 11, 75, 38,144,224,211, 35, 92, 73,146, 12, 43,193,
95, 4,229,218,201,219,227,188,173,119,159,112, 52,122, 33,107,
232, 83, 23,181,182, 13,156,166,208,254,160,251,231,226, 36, 96,
185, 34,220,184,117,253, 87, 89,213, 53, 58, 71,186, 22,169,247,
104, 16, 44,237,240,116,101,105, 31, 99,203, 28, 3,207,165, 72,
51,161,127,205,204, 85, 24, 82,190,245, 41,187,103,130, 47, 25,
221,133, 66,147, 55, 40, 5, 59,174,244,242,222, 79, 30, 94,175,
151,228,164,241,148, 97,102,246,250, 84, 90, 65, 76, 54,129,152,
6,216, 46,209,183, 69,157, 20,199, 86, 62,118,170,138,168, 27,
230,154,100,198, 29,114,115,167,120, 49, 68,248, 2,200,108,243,
109,255, 39, 60, 50,234,180,202, 74, 45, 70, 91,197, 18,110,194,
184,220, 92,157,252,195, 33,122,151, 99,194, 29,105, 98,110, 95,
89, 65, 39,242,232,167,148,182, 97,177,135, 69, 32,253,179, 16,
77,226, 78,134, 64,202,149,230,178,207,136,203,168,190,206, 0,
86, 12, 40, 60,102,196,162, 47, 34,200,180, 1, 44, 79, 17, 53,
204,222, 19,237, 93,120, 48,250, 73,224, 62, 43,198, 61,249, 85,
181,161,163, 37,112,213,212, 80,132,189, 26, 8,216,201,138,255,
193, 22, 68,116,144,225,246,131, 91, 52,231,241, 70, 18, 31,247,
248,154, 96, 10, 72,209,121, 13,156,219, 14, 71, 3,104, 15, 59,
175,139,188, 84, 82,208,166,158,171,123,140,108,127, 76, 75,186,
83,191,111, 50, 21,221,114,128,117,199,174,152,142,109,103, 7,
159,141, 67,173,124,254,211,187, 11, 63,100,214, 58, 6, 88,239,
228,183,223,205,236, 30, 20,169,126,146, 49,176, 56,155, 35,133,
229,145,251, 74,233, 9,137,217,119,244,147,118,150,153,115,125,

197,185, 90, 81, 2, 54,192, 24, 5, 28,238,218, 66, 46,130, 38,
245,215,243,210,113, 25, 23, 51,164,143, 55, 94,227,234, 87,106,
57, 41,107,165, 36,235, 27, 42,129,170,101, 45,160,240,172, 4,
69, 11, 57, 7,218,127,232, 59,105,166,133,213,159, 29, 78,163,
0,212, 63, 28,229,206, 92,107, 17, 13,142,205,248, 56, 34,100,
181,221,223,176, 90, 83,143, 39,179,188,130, 77,164,108,150,207,
24, 99,240,185, 94, 3,239,134,247, 55, 12, 52, 5,146,157,148,
252,154,235,118,219,186, 44,101, 18,198, 51,167, 4, 82,234,253,
203,187, 91,197, 20, 42, 21, 73,231, 67,145,153, 33, 32,106, 53,
147,109,115,246,183, 88,104,245, 64, 50,128, 48,243,102,241,190,
189,171, 93, 46,193,136, 49,250,116,131,209, 87,175,119, 61, 19,
125,151,137, 31,165, 62,161,251,174, 16,210,216,121, 84,227, 15,
226,204,238, 76,135,230,113, 98,208,195,249, 72,192,158,160,236,
156, 66, 35,228,255, 97,123,201, 45, 96, 75,222,211,122,217, 38,
89,170,237,141, 36,124,162,114, 58, 74,199, 8, 41,112, 80,139,
178,244, 1, 70,184, 47,155,152, 65,138, 22,220,191, 26,202, 10,
120, 6, 25, 54, 40,169,144, 30, 14, 60,129,194, 43, 27, 79,233,
68,242,177,149, 9,224,132,180, 85,214, 86,117,225,172, 37,140,
126,215,173,200, 81, 23,182, 2,110,111,103,196,254, 71, 95,168,
149,196,139,185,214,109,183,170,126,122,133,248,232,244, 93,157,
236,237,140, 9,217,137,150,107,239, 54,111,176,104,114,242, 66,
4,234,159,174,252, 46, 43, 86,223, 1,120,231, 84, 48,195,156,
91,132,188, 45,152, 55,130, 74,184, 36,125, 10, 88,179,202, 7,
249,215,203, 94,213,171,112, 98, 19,158, 6,253,110,115, 28, 23,
77, 80,205,189,233, 97,168,143,250, 30, 18,192,246, 58,208,147,
186,161,124, 72,206,190, 63, 64, 61, 41,105,102,251,128, 79,194,
219, 35, 59, 15,180, 8,247, 96,172,209,200,164,240,235, 31,191,
162,146,117, 85,177,106,226,229,155,169,222, 21, 71, 0, 95,116,
163,228,212, 3,182, 49,144,210, 11,138, 60, 38,173,118,165,127,
100,245,166,119,101,178,145, 70,199, 78,224, 73, 16,225,211,148,
181,201,134, 13, 17, 52, 14, 47, 90,230, 44,241, 69,151, 53,187,
42, 34, 76, 33,193,198,220,227,204, 82, 89,254,121, 25, 12, 67,
40, 62, 27, 39,153,113,197, 65, 24, 75, 81, 5,167,141,207, 83,
255, 26, 56,103,238, 20,154, 92,136, 2, 37,123, 50,243,160,131,
51,129, 99, 68,221, 22,142, 57,108,175, 87,216, 32,218,135, 29,
76, 10, 49, 17,220, 3,196,117, 67, 46, 48, 79,171, 51, 25, 30,
0,148, 56, 44,255,199,211, 55,115,161,210, 45,160,120, 37, 24,
100, 97, 33, 22,163,130,152,147,207,236,150,123, 36, 71,222,201,
102,125, 84,141,116, 73, 38,200,213,109,252, 9,215,158,205, 63,
245,185, 64, 27, 99,253,195,242,217,244,223, 74,227,110,167, 78,
8,138,126, 32,247, 34, 23,231,188,191,238, 70,106,225, 83,214,
2,190, 12,206, 94,105,240, 75,124,184,221,165,157,151,143,219,
212,164,168,197,251, 15,182,129,166,194, 42,193,172, 69, 29,232,
235, 86,122,113,239,233, 26,186, 91, 88, 1, 50,135, 53, 35,127,
7,254, 6, 61, 54,181,204, 11,118,183,114,103,149, 59,208, 93,
18,187,111,248, 41,131,250,180, 65, 87,234, 81,175, 95, 80,202,

39,162,132,189,112,153, 19,209,203,216,174, 98,237, 47, 52, 96,
14,243,142,241,107,104,173,133,121,198,169, 13, 85,146,145, 60,
228, 57,224,226, 16, 5,139, 68, 72,154,229,155, 89, 90,101,144,
246,134,218,156, 43, 82,119, 66,136, 77,159,179, 4,176, 31, 40,
58, 92,178, 62,249, 28,108,137,192, 20,170, 21,128,177,230,140,
156, 57, 82,101, 47, 40,153,171,223,185,230,253,166, 26,150, 33,
169, 72, 12, 43,168,247, 86,182,177,131,167, 96,196,172,154, 10,
37,192,251, 62, 71, 61,179,176,163, 85, 69,204,121,161, 90, 27,
103,203, 58,221,142, 0, 35,250,188,151,107, 51,248, 23,148,147,
80,224,212,126,181, 3, 83, 63, 67,140, 5, 4, 24,152, 46,243,
70, 50, 49,236, 6,141,209,109,127, 93,208,252, 34, 88, 28, 65,
222,111, 68,249,123, 55, 1, 64,159, 76,143, 17,175,227, 66,239,
173,120,190,164,145, 91,244, 30, 2,228,232, 14,180, 87, 8, 75,
218,174,178, 15, 29,219,246, 89,104,137,191, 53, 60,216,200,113,
245,238,217,132,108, 94,124,119, 59,149,205, 45, 31,158, 74,255,
193, 73, 39, 13, 56,135, 95,184,235,189, 52,122,240,112, 98, 54,
226,233,130, 79,202, 77,187,215,160,102, 38,206,231, 9,144,234,
197, 21,110, 32, 81,207,134, 20,170, 11, 18,155, 36, 41,157,183,
138,220,213,136,254,162,125,105,198,133,115,201,100,106, 92,165,
128, 99,242,139,225,194, 7, 16, 48,117, 19, 84,229,199, 42, 78,
211,146,186,118,114,116, 22,195,210,241,237, 97,129, 25, 44,214,
153, 32,121,224, 26,235,190,175,106, 77, 88, 47, 1, 33,251, 99,
129,242, 63,170, 19,105,123,187, 49,244, 55,233,210,165,225,228,
207,118,181, 7, 75,109,182,226, 40, 25,239, 42,144, 2, 78, 37,
185,147,229, 96, 5,145, 66,191, 84, 0, 48, 65,171, 31,248, 68,
119, 54,127,172,232,142,133,154,209, 86, 53, 74,116, 85,201,206,
204, 58, 87, 60,166,200,227,124,208, 28, 24, 73, 34, 51,222,146,
120,247, 91,179, 16, 83, 50,255, 76,231, 80, 95, 18,134, 46,198,
243,104,250,151, 29, 52, 23,211, 79,130,238, 9, 30,128,221, 61,
103,240,122,186,152,254,246,164,102,234,137, 8,219,107, 56,110,
108,159,214, 20,126,174,139, 62,196,160,135,177,223, 93,143,101,
136, 3, 10,195, 81,178, 64,217, 36,203,180,138,199, 57,237, 41,
176,155, 38,162,253,241,114, 82,158,111, 97,202,192, 17,168, 39,
148,249, 12, 98,161, 72,169,236, 90, 11,156, 6,216, 35, 69, 89,
112,218, 94,188,163,194,220, 27,189, 22,197,193, 14,252,167, 43,
71, 21,212, 13, 44, 59,131,183,113, 45,245,115, 70,150,100,205,
4,230,173,141,215,149,157,132,117,213,125, 92, 67, 15,184,140,

S[6]

223, 26,254,113,159,245,233, 87,114, 99,140,102,168,169,206,187,
 88,138,214, 69,155,112,178, 98,100, 1, 48,192, 60,198, 86,215,
 219, 93,240, 97,132,228,200, 8, 34,189, 70,193,164,253, 66,225,
 105, 33, 74, 25, 96,142, 16,157,149, 22, 10,255,229,190,222, 63,
 144,230, 5, 84,217, 82, 73,148,241, 27,152, 92,246,195, 30,139,
 20,167,121,181, 7, 91, 9,209, 49, 15,242,221,211,226,177, 78,
 47,237,163,179, 23, 42, 57,151,188,147,234, 68,203, 59,118,250,
 109,136,175, 85, 75,117,104,130, 43, 17,120, 32,191, 58,176,110,
 194, 90,199, 81,146, 12,143,129, 18, 0,108,171,216,174,201,115,
 13,131, 95,185,160, 37,220,119, 6, 53, 11, 24,213,183, 19,107,
 247, 36,123, 38,236, 52, 28,182,103, 62,249, 64,170,197, 65,106,
 150,135, 72,173,133,208,125,251, 71,165,141,154,205,161,158, 51,
 244,248, 76,137, 21, 89, 4, 67, 2, 83,128, 45,224, 46, 41,252,
 227,196, 56, 61,166, 80, 29, 39,101,134,162, 55,235,180,231,156,
 35,122,232, 79,204, 44,116,212,202,153,243, 50,145,184,239, 54,
 111, 40,124,172,186, 31,126, 3, 94,238,127,207, 77, 14,218,210,
 212,136, 19, 33,195,103,104, 29,208,241,242,140, 95, 34,228, 82,
 165,184, 90, 24,154, 28,236,102, 83,227,139,145, 71,222,215,112,
 217, 1, 5, 81,155,109, 54,120, 76,119,243, 50, 88,164, 96,213,
 159,116,117,175, 74, 99, 18, 55, 44, 12, 79,105, 39,106,187, 80,
 128,235, 22, 66,107, 97,207, 68,171, 30, 36,149, 31,229, 3,153,
 176, 70,191,246,166,150,179, 7,182, 43,206,158, 16,141, 93,148,
 115,123, 23, 86, 42,249,180,193,167, 85, 38,126,202, 40,211,178,
 10, 27,181,129,189,226,170, 98,250,173,110,219,122,223, 11, 51,
 132,239, 4,156, 47,147,138,232,194,111,252,174,200, 14,214,118,
 8,143,254,125,198, 32,134, 94, 9,255,196, 78, 53, 17,224, 61,
 162, 84, 15, 57, 89,172,216,185,218,201,233,142,131,210, 20,204,
 221,183,248, 35, 2,237,135, 64,124, 48, 59, 0,230, 62,177,100,
 26, 41,238,163, 45,225,108,203, 52, 72,151, 58, 75,121,152,192,
 6,240, 25,251,186, 87,253, 69,197,234,144, 77,160, 46,146,245,
 49, 21,188,137, 91,247,220,190,127, 63,157,169, 67,244, 37,231,
 161, 65,133,130,209, 13,114,199, 73, 56,168,101, 92,113,205, 60,
 217,198, 61, 81,212, 41,112,109, 11,213,152,113,144,162,220, 66,
 194,110,123, 72,238,151,224, 40,139,205,177,170, 96,229,105, 4,
 12,214,218, 13,200, 97, 28,126,155, 69,209,208,179,133, 31, 22,
 148, 5, 17, 2, 24, 89, 30, 9,163,243,159,149,254,124, 27,154,
 188, 64,244,193, 18,216, 86,242, 78,233, 7,119, 8, 44, 65,234,
 158, 54,221,206, 48, 47, 58,251,210,135,104,228, 74,117,235,196,
 32,156,183, 79,178,169, 42,164, 88, 60, 80,203,146, 62,142,145,
 187, 98,182, 50,141,136, 77, 85,132,215,211,116,111,150, 76,189,
 33,120,241,190, 3,181, 0,128,253,201,199, 39, 49, 16,167, 94,
 184,185,137, 15,195,223, 82,100,157, 37,103, 51,122,239, 19,246,
 10, 45, 38,173,114, 87, 70,121,168,197, 84, 29,175,252, 71,236,
 83, 55, 56,219,250,143, 68, 14,118, 6, 99,102,232,222,161,153,
 130,160, 63, 26,249,230,129,248,108, 67,134,247,227,140,255,138,

231, 1,245, 21,125, 36,172, 57,106,225,171,186,237,115,207, 52,
91, 90, 25,202,107,204, 34, 75, 46,180,101, 20,166, 23,226,147,
240, 53, 95,174,192,131, 93,176, 43,165,191,127, 92, 59, 73, 35,
188, 31,239,121,133, 7,204, 52,246, 27,124, 66,162, 65,146,132,
22,103, 97, 12,108,170,167,211, 87, 71,113, 11,240, 24, 41,215,
236, 59,134,163,185,232, 35,150, 13, 29,237,219,173,217,110,158,
119, 90, 55, 50, 4,250,243,206,104,205,220,139, 68,164,213,168,
176,127, 28,234,126,222, 5, 39,233,231,151, 57, 16, 34, 48,142,
244, 78, 21,218,200, 3,141,153,186,190,149, 38, 64,171, 73,174,
207, 94, 76,157, 46,180,247,223, 45, 30,112,187,155,116,241,137,
203,140, 79,253, 32, 18, 51,160,100,154, 72, 9,202,147,122, 47,
6,184,182, 99,159, 10, 83, 49,107,181,238,197,242,192, 82, 74,
131, 36, 1,245, 75,175, 2,136, 92, 25, 42,118,194,228,255,225,
70,172,214, 17, 53,130,165,189,123,138,208,117,224, 80,254, 81,
201,249,143, 8,144,125, 19,252,177,227,212,210,216,101,129, 95,
251, 54,196, 67, 89,111,102, 96,235, 20,135,114, 15,221, 61,191,
148,105, 44,195,179, 0, 86, 14,193,109, 40, 88,169, 77,120,199,
156,161,166,115,209, 60, 37, 85, 56,198, 84,128, 62, 43,152, 26,
183,145, 69, 23, 58,248,178, 98, 33, 91,229,226, 93,230,106, 63,
152,162, 58,157,212,172, 75, 13,139, 48, 39, 9,119,121, 96, 37,
69,101,242, 73, 17,148,217, 59,122,207,177,237,240,224,116,198,
109, 70, 4,127,128,103,137, 87, 11,156,153,125, 67,129, 84, 12,
208,194, 52, 71,186, 36, 8,190, 0,146, 92,115, 86,196,144, 32,
111, 28,202,100, 38,197,251, 15,102, 49, 93,183,159, 18,209,225,
56, 41,176, 2,150,248, 44, 99,169, 25,193,249,226, 89,228, 45,
211,246, 1, 10,126, 21, 74, 3, 6,185,192, 22, 64, 78, 77, 27,
164,236,252,254, 95, 65,107, 79, 54,140,199,189,149,133,187, 20,
180, 91,232,195,191,188,147,106,158, 34,151, 63,233, 47,230,154,
184, 85,117,201,104,134, 97, 30, 88, 24,204,142, 46, 33,235,253,
51, 57, 40,138, 35,238,168, 7, 42,171, 76, 19,114,113,165,141,
66,203,167, 80, 62,160,219,132, 43,223,178,155,229,214,173,123,
53,213, 5,161,120,250, 81,131,200,255,234,247, 26,124,145,170,
55,245,110, 68, 14, 90,175,179,244, 31,108,227, 50,105,163,205,
83,220,181,143,174,182,135, 72,136,215,166, 16,206,239, 23, 98,
61,112,218,118, 82,222, 29, 60,221,243,241,210, 94,231,130,216,
53,117, 38, 33,242, 26,111, 14,132,119,166, 72, 22, 76,250,204,
157, 96, 70,176,222,206,211,151,134, 90,156, 79,246,109,195,108,
252,142, 84,139,200,235,152,146, 2,226, 12, 89,238, 35,159,198,
229,106,191,164, 3,118,141, 71, 4,201, 95,241, 60,184,161, 41,
223,136,126,103,174, 39,144, 91,243,101,190,215, 46, 65, 55,212,
137,240,172,202, 44,100,216,165, 18,225,125,181,104, 82, 13,209,
231, 0, 21,203,113,138,247,253, 58,175,227,213,116,160,127, 64,
218, 61,149,205,214,192, 37,244,236,171,135, 77, 45, 31, 99,150,
199, 8, 67,230,173, 34,179, 62, 11,234,224, 47,168,197, 94, 28,
194, 88, 68, 87,154, 5, 16, 32, 66,169,145,245, 57,220, 92,163,
69,158, 83,228,183,255, 50,147, 43,237,112,153, 98,167,178,188,

162,217,115,131, 73,140,123, 9,128, 6,170, 30,122, 54,148,251,
19, 23, 59,233,207,248,193,254, 36,210, 48, 52, 20, 29,189, 86,
249,185,232,129, 56,219, 93, 40, 25,120,121,208, 27,187, 17, 15,
24,105, 78,133, 42, 81, 80,155, 85, 10, 51, 75,239,221, 63, 49,
110,130,177, 97, 1,196,102,186,182,114,107,124,180, 7, 74,143,
149,217, 15, 27, 59,225,213, 46, 54,120,252,101,153, 10,244, 49,
89,254,106, 16,235, 69,253,131,102, 39,128,204,247,173, 87,148,
142,151,240, 92, 60, 56,157, 77,126,228,178, 95,165, 1, 25, 91,
140, 90, 17, 37,209, 55, 52, 41, 63, 76,162,199,238,196, 98, 53,
9, 2,203,164,169,231,137,170,186, 58,107,109, 83,174,114,221,
68,246, 24, 3,145, 47,180,168,194, 85,212,146,132, 82,110,177,
81,125,147,191,200,241,206,201,117, 23,159,152, 11, 28, 8,187,
31, 70,227, 18,188,123, 30,236, 6,160, 34,245,111,105, 33,226,
104,103,237,130, 19, 74,249,172, 4,216,118,129,171,205,185, 50,
127,135, 42, 99,144,198,124, 5,150,139, 12,161,175,163, 93,208,
223,108,229,207, 72, 14,210,181, 38, 88,115,121, 73, 97,183,230,
122,242, 94,167, 62, 61,158,134,133, 0,219, 80,233,215, 7,197,
29,234, 36, 43, 48, 75,119, 44,250,100,155,141, 20,113, 96, 35,
222,143,195, 79,176, 45,202,220, 66,232,154,179, 71, 26,189, 13,
112,136,193,184, 78, 64,243,138, 22,182, 67,156,251, 86,192,116,
239,218,211,190, 65,166,255,214, 21, 84,224, 57, 51, 32, 40,248,
178,251, 17,103,139,125,230,120,153, 70,114,225,104,172,124,161,
39, 88,222, 91, 59, 0,174,221, 14,220, 76,137, 22,102,107,160,
131,214,176,206,250,217,110, 52,166,215, 12, 64, 21, 78,255,246,
138,242,170,134, 34, 58,142,128,127,156,200,213,191,101, 37, 55,
56,235,179,146,148,239,117, 69, 60,187, 98, 6,154, 81,173, 97,
158,199,232, 80, 4, 86, 44, 84,201,189, 31, 5, 7,144, 25, 66,
244,234,171,126, 10,122, 16, 49,165,159, 9,209,196,203,129,132,
28,228,112, 29,195,147,224,175, 19, 15,229,197,204,236,123, 45,
33,121,163,141, 99,100, 68,194, 87, 95,240,119,111,207, 46, 40,
243,169,212, 89, 13,247,227,219, 92,238, 74,254, 61, 77,152, 30,
241,184,113,143,218, 82, 75,105, 62,237,211, 41, 72,140, 73,157,
188,130, 20,192,109, 57,198, 27, 79, 8, 67, 43, 51,167,249, 1,
135,202, 83,149,118,115,193, 90,253,205,186, 93,181,208,233, 2,
185,164,150, 36,231, 50, 54,183,145,108, 85,116, 11,162,182,252,
26,226, 71,177,223,151, 53,180, 24, 35,155, 63,168, 94, 32, 48,
18, 96,248, 23,133,106,190, 65,245,210,136,216, 42, 47, 38, 3,

S[7]

120,237, 12, 46,124,114,206,196, 72,172,180, 83, 40,154, 68,162,
211,131,137,233,144, 23,173,195, 67,232, 91,186,199, 57, 74,133,
29,166,153,219, 6,204,170, 13, 66, 14,140, 84, 9,203,215,104,
63,245,163, 75,175, 70,253,218, 76,194,197,113, 4,145,209,122,
10,228,221,132,255,234,177, 99, 53,235,216,121, 2,158, 25,225,
44,147,161,244,159,127, 32,183, 1,110,151,247, 47, 27, 73, 18,
128, 11,191, 89, 20,116, 90, 17,217,118,142, 82,184, 15, 94,236,
108, 50,200,249,239,155,134, 69, 28,126, 34, 43,146, 79, 24,251,
88,168,135,143,220,202, 3, 55, 87,207, 52,125, 78,198, 54, 64,
21,111,138,242,106,105,109,123, 36,169,148, 85, 97,189,224, 62,
167,229, 16,119, 39,174, 49, 98,176,240,150, 48,187,250, 80, 0,
22, 8,230,241,139, 37, 42, 95,130,208,243, 65, 81, 93,160,157,
115,192,100,156,188, 51,222,149,213,223,182, 59, 71,212,164,231,
238,190, 7,102,226, 35, 77, 45, 86,178,254,227, 60,136,141,252,
152,101, 38,214,112,165, 5,171,185, 41,117,248, 92, 61,129, 33,
96, 56,210,193, 19,103,201,107, 31,205,181,246, 26, 58, 30,179,
63,166,193, 54, 90, 27,151,107,120, 56,139,147, 81,229,221,210,
58, 31,104, 3, 72,149, 84, 32, 26,182,244,186,161,154,106, 98,
7,162, 24, 2,175,155,203, 66,156,122,190, 17,197, 37, 36, 25,
61, 77,134, 79,201,117, 23,124, 11,132, 47, 33, 39,195,200, 75,
237,220,140,217,160,103,219, 96, 99,222,248, 4,230, 89, 20,194,
119,178,187,252,113,171,238, 22, 30, 80,141,253,216,112,218, 69,
176, 18,191,138, 60,205,137, 83,247,250,211,144, 40,207, 64,168,
231,208,125, 34,235, 55,150,128,209, 14,116,243, 1,110, 21, 45,
85,223,224,121, 86, 78, 91, 92, 76,183,227,233,102,245,174,255,
158, 57,215, 8,108,167, 51, 59,163,101,228, 53,236, 28,123, 42,
38,204, 87,130, 95, 50,180,164,126,157,152, 5,170,179,100,159,
41, 46, 74,206,192,246, 6,143,188, 52,251,105,196, 35,242,145,
88,234,184, 13,111,214, 0, 19,177,226,135, 16, 73,148,189, 29,
12,129, 9, 43,115,118, 15,172, 70,213,131, 93,142,202, 71, 82,
67, 94,232,165,212, 48, 49, 44,241,169,198,249, 68, 97,114,133,
173, 65,239,109,146,225,153,181,240, 10,185, 62,136,254,199,127,
89,251,192,217, 33,106, 73, 83,204,218, 45, 32, 84,182, 18, 52,
51, 3,178,153,199,147,244,151, 97,177, 93,216,170, 57, 31, 37,
5,167,175,114,172,131, 63,162,208, 23,146,185,156,126, 1,117,
6,165, 20,164,253,186,255, 28, 92,174,181, 67, 7,144,107,160,
25,235, 39,225,124, 2,118,210, 50, 75, 29,128,136,135,228,188,
205, 13,201,169,119,155, 43,127, 71, 60, 80, 0, 19, 76,220,221,
34, 17,120,121, 35, 66, 82,105,229,224, 38,202,231,138, 99,233,
46,247, 95,239, 10,197,226,145,104,252,137, 59,168,159, 47,211,
242, 61, 53,212,166,190,214,122,222, 8,194,254,130,209, 70,191,
158,143,132,103,112,206, 98,102, 42,245, 88,198,150,241, 87, 74,
246,195,250,215, 36, 85,157,149,161,108,183,141, 48,129,148, 81,
78, 58,236,101,189,223, 96,187,227,238, 27,240,179, 26,180,139,
4,125,203,219, 90, 86,248, 44,249,173, 9,109, 68, 22, 62, 15,

24, 94, 21, 12,207, 49, 65,154,140,171,234, 40,113,176,230, 14,
56,123,213,142, 30, 54,184,243, 11,134,232, 77, 55, 41,237,193,
133,115,111,152,163, 79,116,196, 64, 91, 72,200, 69, 16,100,110,
10, 52,146, 15,250,206,232,244, 85,116,172,205,134,190,136, 55,
107,185,126,156, 50, 34,178,229,231, 24, 94, 72,180,241, 53,194,
243, 4,181,162, 28, 86, 69,204,196,128,251,233, 35,140, 46,104,
48,248, 8,161, 27,195, 20,236,198,183,253,188, 29,166, 42,171,
3, 76, 38,150, 51,164,119,149,201, 92,108,111, 18, 56,210,207,
124, 98,228, 88,192,120, 33, 1,218, 58,182, 80,221,138, 73,202,
31,105,169, 68,212,118, 78,153, 37, 74, 30,224, 64, 26, 89,174,
79, 23,247, 12,155,145,208, 62,152, 13, 5,158, 71, 95,135,193,
254,227,129, 65,200,167, 60,213,170,160, 21,122, 97,131,238,121,
113,163, 11, 99, 82, 6,230, 2, 32,197, 49,142, 59,226,123,222,
91,246, 39, 67, 47,216, 7,186,112,214,125,103,144, 83, 25, 14,
9, 93,191,168, 19, 75,239,114,237, 43, 77, 45, 66, 41,130, 0,
165, 22,179, 36,255,235,147,102, 61,117,139,127,240,249,143,176,
101, 81,133,177,215,217,132,203,199, 44,189,245,159, 87,141, 70,
242, 96, 63,109,175,184,148,225, 54,115,234,154,252,209, 57,151,
211,220,187, 90,106, 84,137, 17, 16,110,223,157,100,173,219, 40,
235,187,254, 59,131,125, 56,145,236,110, 63,129,144, 83, 66,168,
132,135, 71,255,193, 92,134, 18, 25,133,117,137, 14,208, 10,103,
51,151, 74, 75,172,185,140,179, 0,101,104,194,228, 22,136,107,
70, 64, 76, 35, 95,198,148, 62,163,152,105, 99, 41, 78,161, 2,
166,106,248,176,189, 27, 39,188,246,201,200,209,224,197,205,175,
162, 98,215,239,150, 84, 11,182, 65, 53,183, 72,147, 42,251,202,
170,212, 21,113,218, 9,206,243, 13,213,237,249, 8, 40, 5, 12,
181, 73,225,123,122,207, 6,167, 46,164,229,121, 87, 60,244, 57,
146, 81,149, 28,157, 61,210,155, 96, 1,233,174,240, 29, 58, 93,
211, 30, 4,231,108,222,216, 31,253, 33,159,139,190,173,102, 54,
36,156,171,214,154,227, 85,186, 55, 48,203,223,138,178, 52,100,
192,199, 79, 37, 34,250,247,120,109, 24, 23,245, 44, 88,141, 20,
80,112, 67,127, 90,195,169, 68, 86,128,230,118, 45, 47, 3, 38,
143,217,220, 49, 17, 91, 94, 7,165,126,124, 77,142,191, 43,160,
226,238, 69, 15,196,114,130, 32,252,242, 19,232,153, 50,158,221,
111,241,116,234, 89,115, 26,177, 97,184, 16,204,180,219,119, 82,
203,184, 98, 96,188,174, 72, 54, 58,230,250,111, 84,255,192,120,
78,164,221,135,100,196,153,227,198,183,177, 10, 70,254,235,169,
211, 48,109,237,161,207,219,159,172,239, 74,122, 77, 56, 22, 62,
117,216, 95, 17, 75,236, 41, 15,119, 13,102, 27, 53,225,101,240,
168, 39,154,226,189, 40, 20,176,175,247, 32,238, 4,150,156, 93,
1, 81,143,252, 16,178, 83,180,107,133, 12, 31,157,200,187,142,
38,197,195, 8, 97,190,139,163, 80,232, 50, 24,204, 64, 47,141,
126,138,234, 6,215,151, 91,136,181,210,182,253,130,218,248,242,
68, 34,194, 57,231,125, 18,186,115,222,137, 76,166, 65, 66,140,
199,113, 49,171,229,103,213,124, 23,165, 37, 5,220,202, 86, 3,
208,217, 73,144, 29,162, 25, 26, 51, 7,118, 28, 30,127,110,173,

129,116,132,146,145,134, 21,212, 59, 79, 43, 67, 11,206,251,105,
106,223,158,123, 9,245, 63,147, 46, 92, 19, 90,244, 60,224,185,
193,214,108, 69,128,228,246,152,179, 88, 99,249, 55,191, 85,112,
149, 61,104,121, 87, 42,201, 14, 89,243,233,148,209,205,167, 45,
36, 0, 52,114, 71,241, 82,170,160, 35, 94, 44,155, 2, 33,131,
127,148,142,186,239, 55,168,144,241, 95, 75,143,176,135,225, 37,
128,214, 73, 78,109,204,150,170,110, 94, 67,174, 66, 62,123,221,
76,120, 60,114,190,160,254, 81,220,167,159, 69, 61,130, 58,105,
191, 40, 84, 59,158,111, 11, 33,255,228, 72,177,215, 44,209, 99,
49,118, 24,162,104,219,182,240,185,166,155,178, 41,243, 5, 88,
203, 14,232,230, 34, 42,146,216,205,236,113,115,196,165, 56,210,
172, 92, 39,233,202,199,154, 57, 21,134, 31,137, 48,116, 85, 13,
22,223,106,117, 97, 65,145,207,126, 0,136,212,183, 28,242, 45,
54,245, 16,131,180,238,201,231, 83,129,124,152, 38, 18, 36,192,
229,173,149, 71,138, 23, 89, 30,169,121, 86, 50,140,206, 2,181,
139,107, 20,246,112,179, 3,133,208,251,197,226,235,244,224,217,
193,101, 9, 35, 74,132,227, 70,234, 91,102,194, 98,164, 79,189,
200,222,211,156,250, 43, 26, 93,122, 96, 68, 64,175,248,119,171,
8, 1, 77,188, 46, 10,253, 51, 52, 15,198, 6,125,151, 4, 12,
47,141,213,163, 27,147, 17,103,187,108,249,247, 32,161, 82, 63,
53, 25,218,100,237,184, 80,195, 90,153, 87,157, 7, 19, 29,252,
225, 29,198,167,178,235, 76,210,171,181,131, 35,130,209, 71,213,
184,230,127,123, 80, 7,190,144,147,254,183,212, 5, 18, 57,255,
93, 48,132, 1,101, 45,137,135, 90,193, 77,143,176,251,113, 86,
239, 81, 16,128, 30,170, 13,247,236,111,121,217,182,156,133,175,
157,186, 47,134, 94,244,189,108,194, 0,165, 19, 85,159,237,211,
33,228,166, 62, 42,248,149, 8,252,195,253,107,188,206,191, 32,
6,103, 58, 83, 38, 96, 63, 9,102,119,242,202,207,122, 26,196,
36, 53, 68,120, 74, 79,161,118,148,158,162, 82,136, 3, 51,117,
125,199,129,139,240,234, 78,224, 52,232, 28,220, 39,141, 4,241,
87,126,138,243,115,145, 21,177,163, 37,226,146,173,216, 41,140,
11, 54, 50, 44, 75, 40, 67, 72,100, 43, 17, 23,215,219, 64, 49,
2,169, 69,250,124,238,205,221,246,229,172,233,114, 24,249, 84,
31,150, 97, 92,218,179, 59,214, 89, 10, 25,151,245,112,197, 20,
153, 27,200,116,106, 34,109,152, 91, 60,192,187, 22,110,154,231,
46, 88, 95,185, 66,208,223, 61,180,104, 12,168, 55, 98,105,160,
73, 99,142, 14,204, 15, 65,222,164,203, 70, 56,174,227,155,201,

Appendix C: Pairs-XOR tables

Table 4: ES0/S0 High-Probability XORs

Input XOR	Output XOR	Probability
X'054F'	X'E9'	2.15E-5
X'0DAD'	X'17'	2.06E-5
X'0DAD'	X'B8'	2.06E-5
X'6635'	X'97'	2.06E-5
X'700E'	X'17'	2.24E-5
X'700E'	X'B8'	2.24E-5
X'7B13'	X'97'	2.15E-5
X'81CB'	X'DA'	2.06E-5
X'8233'	X'4D'	2.06E-5
X'FD28'	X'97'	2.06E-5

Table 5: ES1/S1 High-Probability XORs

Input XOR	Output XOR	Probability
X'03D1'	X'84'	2.06E-5
X'942F'	X'0A'	2.32E-5
X'9816'	X'2C'	2.15E-5
X'D3CE'	X'68'	2.15E-5

Table 6: ES2/S2 High-Probability XORs

Input XOR	Output XOR	Probability
X'228C'	X'32'	2.24E-5
X'28EF'	X'F7'	2.06E-5
X'9826'	X'AF'	2.06E-5
X'DD11'	X'B3'	2.15E-5

Table 7: ES3/S3 High-Probability XORs

Input XOR	Output XOR	Probability
X'87CA'	X'0C'	2.06E-5
X'C8E7'	X'0C'	2.15E-5

Table 8: ES4/S4 High-Probability XORs

Input XOR	Output XOR	Probability
X'6D0C'	X'09'	2.06E-5
X'E33F'	X'C9'	2.06E-5
X'FBF3'	X'AE'	2.15E-5

Table 9: ES5/S5 High-Probability XORs

Input XOR	Output XOR	Probability
X'20F0'	X'AA'	2.32E-5
X'30BB'	X'58'	2.15E-5
X'3DA5'	X'AA'	2.06E-5
X'C1F4'	X'33'	2.06E-5
X'CCAB'	X'AA'	2.06E-5
X'D029'	X'92'	2.06E-5

Table 10: ES6/S6 High-Probability XORs

Input XOR	Output XOR	Probability
X'4E4F'	X'32'	2.06E-5
X'7DA6'	X'F2'	2.06E-5
X'A131'	X'F2'	2.15E-5
X'AA88'	X'32'	2.06E-5
X'FE01'	X'32'	2.41E-5

Table 11: ES7/S7 High-Probability XORs

Input XOR	Output XOR	Probability
X'8BB8'	X'90'	2.06E-5
X'C72C'	X'29'	2.06E-5
X'CC5E'	X'88'	2.06E-5