## One-Time Pad

The sender uses each key letter to encrypt exactly one plaintext character.

Encryption is the addition modulo 26 of the plaintext character and the one-time pad key character.

The sender encrypts the message and then destroys the used pages of the pad or used section of the tape. The receiver has an identical pad and uses each key on the pad, in turn, to decrypt each letter of the ciphertext. The receiver destroys the same pad pages or tape section after decrypting the message.

## ONETIMEPAD

and the key sequence from the pad is
TBFRGFARFM
then the ciphertext is
IPKLPSFHGQ
because
$\mathrm{O}+\mathrm{T} \bmod 26=\mathrm{I}$
$\mathrm{N}+\mathrm{B} \bmod 26=\mathrm{P}$
$\mathrm{E}+\mathrm{F} \bmod 26=\mathrm{K}$ etc.

Binary case:

$$
\begin{aligned}
& \mathrm{x}=0100110101011101 \ldots \\
& \mathrm{k}=1101000011101011 \ldots \\
& y=\quad 1001110110110110 \ldots
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{y}+\mathrm{k}=(\mathrm{x}+\mathrm{k})+\mathrm{k}=\mathrm{x}+(\mathrm{k}+\mathrm{k})=\mathrm{x} \\
& +: \text { mod } 2 \text { addition (XOR) } \\
& \text { Probabilistic model (C. Shannon) }
\end{aligned}
$$

X, Y, K random variable
K has uniform distribution (coin flipping sequence)
X and K are independent

$$
Y=E_{K}(X)
$$

Perfect encryption: $\mathrm{I}(\mathrm{X}, \mathrm{Y})=0$.

Theorem 1: Perfect encryption exists.
Proof: One time pad
$\mathrm{Y}=\mathrm{X}+\mathrm{K} \quad(+=\oplus)$
$P(Y=y \mid X=x)=P(X+K=y \mid X=x)=P(K=y-x \mid X=x)=P(K=y-x)=2^{-N}$
( X and K are independent)

$$
\mathrm{P}(\mathrm{Y}=\mathrm{y})=\sum_{\mathrm{x}} \mathrm{P}(\mathrm{X}+\mathrm{K}=\mathrm{y} \mid \mathrm{X}=\mathrm{x}) \mathrm{P}(\mathrm{X}=\mathrm{x})=2^{-\mathrm{N}}=\mathrm{P}(\mathrm{Y}=\mathrm{y} \mid \mathrm{X}=\mathrm{x})
$$

Theorem 2: $\mathrm{H}(\mathrm{K}) \geq \mathrm{H}(\mathrm{X})$

$$
\begin{aligned}
& \mathrm{H}(\mathrm{X})=\mathrm{H}(\mathrm{X} \mid \mathrm{Y})+\mathrm{I}(\mathrm{Y} ; \mathrm{Y})=\mathrm{H}(\mathrm{X} \mid \mathrm{Y}) \\
& \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) \leq \mathrm{H}(\mathrm{X}, \mathrm{~K} \mid \mathrm{Y})=\mathrm{H}(\mathrm{~K} \mid \mathrm{Y})+\mathrm{H}(\mathrm{X} \mid \mathrm{Y}, \mathrm{~K}) \\
& =\mathrm{H}(\mathrm{~K} \mid \mathrm{Y}) \leq \mathrm{H}(\mathrm{~K}) \\
& (\mathrm{H}(\mathrm{U}, \mathrm{~V})=\mathrm{H}(\mathrm{U})+\mathrm{H}(\mathrm{~V} \mid \mathrm{U}), \mathrm{H}(\mathrm{X} \mid \mathrm{Y}, \mathrm{~K})=0)
\end{aligned}
$$

Corrollary: $\mathrm{H}(\mathrm{X}) \leq \mathrm{H}(\mathrm{K})=\mathrm{H}\left(\mathrm{K}_{1}, \mathrm{~K}_{2}, \ldots, \mathrm{~K}_{\mathrm{N}}\right) \leq|\mathrm{K}|$

Use data compession before applying one time pad encryption!

Consider the case when $|=|=|=|: \dot{:}|=|$ 쎄 , i.e. the size of message space, key space and ciphertext space is the same.

Theorem 3: Assume $\mid$ 대 $=|: \dot{:}|=\mid$ 서 . The cryptosystem is perfect if and only if

A1.) every key is used with the same probability (1/|써 ), and
A2.) for every message $\mathbf{x}$ and cipertext $\mathbf{y}$ there exists a unique key $\mathbf{k}$, such that $\mathrm{E}_{\mathrm{k}}(\mathrm{x})=\mathrm{y}$.

Proof:

1. A1, A2 $\rightarrow$ perfect (similar proof as for Th.1.)
2. perfect $\rightarrow \mathrm{A} 1, \mathrm{~A} 2$ :
perfect $\rightarrow$ for each $\mathrm{x}, \mathrm{y}$ there exists at least one k such that $\mathrm{E}_{\mathrm{k}}(\mathrm{x})=\mathrm{y}$
$|: \%|=\mid$ 써
$\rightarrow \mathrm{A} 2$.
fix y
Bayes th. $\rightarrow \mathrm{P}\left(\mathrm{x}_{\mathrm{i}} \mid \mathrm{y}\right)=\mathrm{P}\left(\mathrm{y} \mid \mathrm{x}_{\mathrm{i}}\right) \mathrm{P}\left(\mathrm{x}_{\mathrm{i}}\right) / \mathrm{P}(\mathrm{y})=\mathrm{P}\left(\mathrm{k}_{\mathrm{i}}\right) \mathrm{P}\left(\mathrm{x}_{\mathrm{i}}\right) / \mathrm{P}(\mathrm{y})$ ( $\mathrm{E}_{\mathrm{ki}}\left(\mathrm{x}_{\mathrm{i}}\right)=\mathrm{y}_{\mathrm{i}}$ )
perfect $\rightarrow \mathrm{P}\left(\mathrm{x}_{\mathrm{i}} \mid \mathrm{y}\right)=\mathrm{P}\left(\mathrm{x}_{\mathrm{i}}\right)$
$\rightarrow 1=\mathrm{P}\left(\mathrm{k}_{\mathrm{i}}\right) / \mathrm{P}(\mathrm{y})$
$\rightarrow \mathrm{P}\left(\mathrm{k}_{\mathrm{i}}\right)$ is constant $\rightarrow \mathrm{P}\left(\mathrm{k}_{\mathrm{i}}\right)=1 /$ 섯.

## Classical simple cryptosystems

1．Shift Cipher
2．Affine Cipher
3．Substitution Cipher
4．Vigenere Cipher
5．Hill Cipher
6．Permutation Cipher
7．Stream Cipher（with LFSR）

## 1．Shift Cipher

敁：：＝奴料
$9 \rightarrow 26$
$\mathrm{E}_{\mathrm{k}}(\mathrm{x})=\mathrm{x}+\mathrm{k} \bmod 26$
$\mathrm{D}_{\mathrm{k}}(\mathrm{y})=\mathrm{y}-\mathrm{k} \bmod 26$
Character conversion（preprocessing）：

| A | B | C | $\ldots$ | W | X | Y | Z |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 1 | 2 |  | 22 | 23 | 24 | 25 |

[^0]attack: exhaustive key search (meaningful plaintext)

## 2. Affine Cipher

## 泎: : 粦

$\grave{k}=\left\{(\mathrm{a}, \mathrm{b}) \in \mathrm{Z}_{26} \times \mathrm{Z}_{26}: \operatorname{gcd}(\mathrm{a}, 26)=1\right)$,
$\cdot{ }^{\prime 2}=26 \cdot \phi(26)=26 \cdot 12=312$
$\mathrm{k}=(\mathrm{a}, \mathrm{b})$
$\mathrm{E}_{\mathrm{k}}(\mathrm{x})=\mathrm{ax}+\mathrm{b} \bmod 26$
$D_{k}(y)=a^{-1}(y-b) \bmod 26$
$\mathrm{x}, \mathrm{y} \in \mathrm{Z}_{26}$

Example:
$\mathrm{k}=(7,3), 7^{-1}=15(\bmod 26)(7 \cdot 15=105=4 \cdot 26+1)$
$\mathrm{E}_{\mathrm{k}}(\mathrm{x})=7 \mathrm{x}+3 \bmod 26$
$D_{k}(y)=15(y-3)=15 y-19 \bmod 26$

## cryptanalysis:

Letter probability distribution in English texts

| lette <br> r | prob. | letter | prob. |
| :---: | :---: | :---: | :---: |
| A | .082 | N | .067 |
| B | .015 | O | .075 |
| C | .028 | P | .019 |
| D | .043 | Q | .001 |
| E | .127 | R | .060 |
| F | .022 | S | .063 |
| G | .020 | T | .091 |
| H | .061 | U | .028 |
| I | .070 | V | .010 |
| J | .002 | W | .023 |
| K | .008 | X | .001 |
| L | .040 | Y | .020 |
| M | .024 | Z | .001 |

## y=FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHV UFEDKAPRKDLYEVLRHHRH

Letter frequency in ciphertext y

| letter | freq. | letter | freq. |
| :--- | :--- | :--- | :--- |
| A | 2 | N | 1 |
| B | 1 | O | 1 |
| C | 0 | P | 2 |
| D | 7 | Q | 0 |
| E | 5 | R | 8 |
| F | 4 | S | 3 |
| G | 0 | T | 0 |
| H | 5 | U | 2 |
| I | 0 | V | 4 |
| J | 0 | W | 0 |
| K | 5 | X | 2 |
| L | 2 | Y | 1 |
| M | 2 | Z | 0 |

R(8),
$\mathrm{D}(7)$,

E,H,K(5),

F,V(4)
$\mathrm{R}(8), \mathrm{D}(7), \mathrm{E}, \mathrm{H}, \mathrm{K}(5), \mathrm{F}, \mathrm{V}(4)$
guess:
$\mathrm{R} \rightarrow \mathrm{e}, \mathrm{D} \rightarrow \mathrm{t}$

$$
E_{k}(4)=17
$$

$$
E_{k}(19)=3
$$

1. $4 \mathrm{a}+\mathrm{b}=17 \bmod 26$
2. $19 a+b=3 \bmod 26$
$a=6, b=19$
(2.-1.: $15 \mathrm{a}=-14=12,15^{-1}=7, a=7 \cdot 12=6 \bmod 26$ )
$\operatorname{gcd}(\mathrm{a}, 26)=2>1$ incorrect guess
next guess:
$\mathrm{R} \rightarrow \mathrm{e}, \mathrm{E} \rightarrow \mathrm{t} \rightarrow \mathrm{a}=13$ incorrect
next guess:
$\mathrm{R} \rightarrow \mathrm{e}, \mathrm{H} \rightarrow \mathrm{t} \rightarrow \mathrm{a}=8$ incorrect
next guess:
$\mathrm{R} \rightarrow \mathrm{e}, \mathrm{K} \rightarrow \mathrm{t} \rightarrow \mathrm{a}=3, \mathrm{~b}=5$ legal key
decryption trial with (check if we get meaningful decrypted text) $D_{k}(y)=3^{-1}(y-5)=9 y-19 \bmod 26$
algorithmsarequitegeneraldefinitionsofarithmeticprocesses
algorithms are quite general definitions of arithmetic processes
result of the analysis: $\mathrm{k}=(3,5)$ is the correct key.

## 3. Substitution Cipher

## 动: = 粦

$\underset{k}{k}=\{$ all possible permutations of the ABC$\}, \stackrel{9}{2}=26$ !
Example permutation $\pi$ : (selected randomly from $\hat{\chi}^{\text {}}$ )

| a | b | c | $\ldots$ | w | x | y | z |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| X | N | Y |  | K | J | D | I |

$\mathrm{E}_{\pi}(\mathrm{x})=\pi(\mathrm{x})$
$\mathrm{D}_{\pi}(\mathrm{y})=\pi^{-1}(\mathrm{y})$
attack (cryptanalysis):
letter frequency
digram frequency trigram frequency

## 4. Vigenere Cipher

Extension of shift cipher (substitution cipher) to a m parallel shifts (substitutions)
$\mathbf{k e y w o r d}$ : key of $\mathbf{m}$ characters (letters): $\mathbf{k}=\left(\mathbf{k}_{\mathbf{1}}, \mathbf{k}_{2}, \ldots, \mathbf{k}_{\mathbf{m}}\right)$ periodical substitution of characters with period m:
the 1 st char. of x is ciphered with the 1 st char. of k
the 2 nd char. ....

| ... | with the 2 nd char. of k |
| :--- | :--- |
| the m-th char. .... | with the m -th char. of k |
| the m+1-th char. .... | with the 1 -st char. of k |

$9 \rightarrow 26^{\mathrm{m}}$
$\rightarrow$ exhaustive key search is not feasible for not too small m

## cryptanalysis:

Step 1.: determination of keyword length m (Kasiski test, Friedman test )

Step 2: finding the shifts (key chars) (Friedman test)

## Step 1:

### 1.1. The Kasiski test:

The idea:
i.) two identical segments of plaintext are encrypted to the same ciphertext, if their distance within the text is a multiple of m ii.) conversely, if we see two identical segments of ciphertext each with length at least 3 chars., there is a good chance that they correspond to identical segments of plaintext

The test: search the ciphertext for pairs of identical segments of length at least 3 , and record the distances. Calculate the gcd of the distances.

### 1.2. The Friedman test (index of coincidences):

Assume we have a string $\mathbf{z}$ of letters of length $\mathbf{n}$, where the frequency of letters (A,B,C...Z) is $f_{0}, \mathbf{f}_{\mathbf{1}}, \ldots, \mathbf{f}_{25}$. The probability $\mathbf{I}_{\mathbf{c}}(\mathbf{x})$ of the event that selecting two randomly selected elements from $\mathbf{x}$ are identical is the following:
$I_{c}(z)=\frac{{ }_{i=0}^{25} f_{i}\left(f_{i}-1\right)}{n(n-1)} \approx{ }_{i=0}^{25} p_{i}(=0.0 .65$ for English $)$
where $\mathbf{p}_{\mathbf{i}}$ is the letter frequency of the actual language for the $\mathbf{i}$-th letter in the alphabet. For random text

$$
\mathbf{p}_{\mathrm{i}}=26 \cdot(1 / 26)^{2}=1 / 26 \rightarrow \mathbf{I}_{\mathbf{c}}(\mathbf{x}) \approx 1 / 26=0.038
$$

The test: Take the letters from the ciphertext at distances $\mathrm{m}=1,2,3, \ldots$ and calculate the index of coincidences for the obtained
substring(m). For the right guess of $m$ index value close to 0.065 is obtained.
Step 2: Finding the key

## Mutual index of coincidences:

Let $\mathbf{z}$ and $z^{\prime}$ two strings of letters with length $\mathbf{n}$ and $\mathbf{n}^{\prime}$ respectively. The corresponding letter frequencies are $\mathbf{f}_{0}, \mathbf{f}_{1}, \ldots, \mathbf{f}_{25}$ and $\mathbf{f}^{\prime}{ }_{0} \mathbf{f}^{\prime}{ }_{1}, \ldots, \mathbf{f}^{\mathbf{\prime}}{ }^{25}$.

The probability of the event, that a randomly selected letter from z is identical to a randomly selected letter from $z^{\prime}$ is the following:
$M I_{c}\left(z, z^{\prime}\right)=\frac{{ }_{i=0}^{25} f_{i} \cdot f_{i}^{\prime}}{n \cdot n^{\prime}} \approx{ }_{i=0}^{25} p_{i} p_{i}^{\prime}$

We have a guess on $\mathbf{k}=\left(\mathbf{k}_{\mathbf{1}}, \mathbf{k}_{\mathbf{2}}, \ldots, \mathbf{k}_{\mathbf{m}}\right)$. Let this guess be $K=\left(K_{1}, K_{2}, \ldots, K_{m}\right)$.

Consider the pair $\mathrm{K}_{1}, \mathrm{~K}_{2}$. Take two substrings of the ciphertext: $\mathbf{z}$ and $\mathrm{z}^{\prime}$, where
$\mathbf{z}$ consist of the letters at positions $1, \mathrm{~m}+1,2 \mathrm{~m}+1, \ldots, \mathrm{im}+1, \ldots$
$\mathbf{z}^{\prime}$ consist of the letters at positions $2, \mathrm{~m}+2,2 \mathrm{~m}+2, \ldots, \mathrm{im}+2, \ldots$.
Calculate the mutual index of coincidences for the pair $\mathbf{z}, \mathbf{z}$ :
$M I_{c}\left(z, z^{\prime}\right) \approx{ }_{l=0}^{25} p_{l-K_{1}} p_{l-K_{2}}={ }_{l=0}^{25} p_{l} p_{l+K_{1}-K_{2}}$

Note: Only the relative shift is important!
Calculate the relative shifts for all pairs of characters of the guessed key (i.e. for $m(m-1) / 2$ pairs). 26 possible keys remain, resolve with exhaustive search.

Homework: Write a program for analysis of Vigenere encryption.

## 5. Hill Cipher



Linear block cipher transforming m character long plaintext into m character long ciphertext by matrix multiplication:
$\mathrm{E}_{\mathrm{k}}(\mathrm{x})=\mathrm{xK} \bmod 26$
$D_{k}(y)=\mathrm{yK}^{-1} \bmod 26$
where the key k is an mxm invertible matrix over $\mathrm{Z}_{26}$
attack (cryptanalysis):
known plaintext attack
$\mathrm{x}=$ friday $, \mathrm{m}=2, \mathrm{y}=\mathrm{PQCFKU}$
$\mathrm{fr} \rightarrow \mathrm{PQ} \quad: \quad \mathrm{E}_{\mathrm{k}}(5,17)=(15,16)$
$\mathrm{id} \rightarrow \mathrm{CF} \quad: \quad \mathrm{E}_{\mathrm{k}}(8,3)=(2,5)$
ay $\rightarrow \mathrm{KU}: \quad \mathrm{E}_{\mathrm{k}}(0,24)=(10,20)$
$\left(\begin{array}{cc}15 & 16 \\ 2 & 5\end{array}\right)=\left(\begin{array}{cc}5 & 17 \\ 8 & 3\end{array}\right)\left(\begin{array}{ll}k_{11} & k_{12} \\ k_{21} & k_{22}\end{array}\right)$

$$
\left(\begin{array}{cc}
5 & 17 \\
8 & 3
\end{array}\right)^{-1}=\left(\begin{array}{cc}
9 & 1 \\
2 & 15
\end{array}\right) \rightarrow \mathrm{K}=\left(\begin{array}{cc}
9 & 1 \\
2 & 15
\end{array}\right)\left(\begin{array}{cc}
15 & 16 \\
2 & 5
\end{array}\right)=\left(\begin{array}{cc}
7 & 19 \\
8 & 3
\end{array}\right)
$$

## 6. Stream Cipher (with LFSR)

$y_{i}=x_{i}+k_{i} \quad i=1,2, \ldots$, where $y_{i}, x_{i}, k_{i}$ are binary variables
LFSR: Linear Feedback Shift Register
Defined by the following linear recursion:
$k_{m+i}={ }_{j=0}^{m-1} f_{j} k_{i+j} \bmod 2, \quad \mathrm{i}=0,1,2, \ldots$
$\mathrm{k}_{0}, \mathrm{k}_{1}, \ldots, \mathrm{k}_{\mathrm{m}-1}$ initial state (random seed)
$\mathrm{f}_{0}, \mathrm{f}_{1}, \ldots, \mathrm{f}_{\mathrm{m}-1}$ feedback coefficients
e.g.
$k_{m}=f_{0} k_{0}+f_{1} k_{1}+\ldots+f_{m-1} k_{m-1}$
$k_{m+1}=f_{0} k_{1}+f_{1} k_{2}+\ldots+f_{m-1} k_{m}$
attack (cryptanalysis):
known plaintext attack
System of $m$ linear equations can be obtained in unknown feedback coefficients.

$$
\left(k_{m}, k_{m+1}, \ldots ., k_{2 m-1}\right)=\left(f_{0}, f_{1}, \ldots ., f_{m-1}\left(\begin{array}{cccc}
k_{0} & k_{1} & \ldots & k_{m-1} \\
k_{1} & k_{2} & \ldots & k_{m} \\
\ldots & \ldots & \ldots & \ldots \\
k_{m-1} & k_{m} & & k_{2 m-2}
\end{array}\right.\right.
$$

## Unicity distance

$$
\begin{aligned}
& K(y)=\left\{K: \exists x, E_{K}(x)=y\right\} \\
& S_{n}=\underset{y \in C^{n}}{p(y)(|K(y)|-1)}
\end{aligned}
$$

Theorem 3: If $|\Sigma 8=|: 9$

$$
S_{n} \geq \frac{|K|}{|P|^{n R_{L}}}-1
$$

where $\mathrm{R}_{\mathrm{L}}$ is the redundancy per letter of the language.

Unicity distance: $\mathrm{n}_{0}$, such that $\mathrm{S}_{\mathrm{n} 0}=0$
$n_{0} \approx \frac{\log _{2}|K|}{R_{L} \log _{2}|P|}$

Example: substitution cipher

Given a cipheetext string of length at least 25 , (usually) unique decryption is possible.


[^0]:    Example encryption：
    $\mathrm{x}=$ wewillmeet， $\mathrm{k}=11$
    $y=H P H T W W X P P E$

