ECE 646 - Lecture 6

Historical Ciphers

Required Reading

- W. Stallings, *Cryptography and Network Security*,
  *Chapter 2, Classical Encryption Techniques*

- A. Menezes et al., *Handbook of Applied Cryptography*,
  *Chapter 7.3 Classical ciphers and historical development*

Why (not) to study historical ciphers?

**AGAINST**
- Not similar to modern ciphers
- Long abandoned

**FOR**
- Basic components became a part of modern ciphers
- Under special circumstances modern ciphers can be reduced to historical ciphers
- Influence on world events
- The only ciphers you can break!

Secret Writing

- **Steganography** (hidden messages)
- **Cryptography** (encrypted messages)
- **Substitution Transformations**
  - **Codes** (replace words)
  - **Substitution Ciphers** (replace letters)
- **Transposition Ciphers** (change the order of letters)

Selected world events affected by cryptology

1586 - trial of Mary Queen of Scots - substitution cipher
1917 - Zimmermann telegram, America enters World War I
1939-1945 Battle of England, Battle of Atlantic, D-day - ENIGMA machine cipher
1944 – world’s first computer, Colossus - German Lorenz machine cipher
1950s – operation Venona – breaking ciphers of soviet spies stealing secrets of the U.S. atomic bomb – one-time pad

Mary, Queen of Scots

- Scottish Queen, a cousin of Elisabeth I of England
- Forced to flee Scotland by uprising against her and her husband
- Treated as a candidate to the throne of England by many British Catholics unhappy about a reign of Elisabeth I, a Protestant
- Imprisoned by Elisabeth for 19 years
- Involved in several plots to assassinate Elisabeth
- Put on trial for treason by a court of about 40 noblemen, including Catholics, after being implicated in the Babington Plot by her own letters sent from prison to her co-conspirators in the encrypted form
Mary, Queen of Scots – cont.

- Cipher used for encryption was broken by codebreakers of Elisabeth I
- It was so called nomenclator – mixture of a code and a substitution cipher
- Mary was sentenced to death for treachery and executed in 1587 at the age of 44

Zimmermann Telegram

- Sent on January 16, 1917 from the Foreign Secretary of the German Empire, Arthur Zimmermann, to the German ambassador in Washington
- Instructed the ambassador to approach the Mexican government with a proposal for military alliance against the U.S.
- Offered Mexico generous material aid to be used to reclaim a part of territories lost during the Mexican-American War of 1846-1848, specifically Texas, New Mexico, and Arizona
- Sent using a telegram cable that touched British soil
- Encrypted with cipher 0075, which British codebreakers had partly broken
- Intercepted and decrypted

Zimmermann Telegram

- British foreign minister passed the ciphertext, the message in German, and the English translation to the American Secretary of State, and he has shown it to the President Woodrow Wilson
- A version released to the press was that the decrypted message was stolen from the German embassy in Mexico
- After publishing in press, initially believed to be a forgery
- On February 1, Germany had resumed "unrestricted" submarine warfare, which caused many civilian deaths, including American passengers on British ships
- On March 3, 1917 and later on March 29, 1917, Arthur Zimmermann was quoted saying "I cannot deny it. It is true."
- On April 2, 1917, President Wilson asked Congress to declare war on Germany. On April 6, 1917, Congress complied, bringing the United States into World War I.

Ciphers used predominantly in the given period(1)

<table>
<thead>
<tr>
<th>Cryptography</th>
<th>Cryptanalysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 B.C.</td>
<td>Shift ciphers</td>
</tr>
<tr>
<td>1586 Invention of the Vigenère Cipher</td>
<td>Frequency analysis</td>
</tr>
<tr>
<td>1863 Kasiski’s method</td>
<td></td>
</tr>
<tr>
<td>1919 Index of coincidence</td>
<td></td>
</tr>
<tr>
<td>1918 William Friedman</td>
<td></td>
</tr>
<tr>
<td>1926 Vernam cipher (one-time pad)</td>
<td>Black chambers</td>
</tr>
<tr>
<td>1919 Invention of rotor machines</td>
<td>Kasiski’s method</td>
</tr>
<tr>
<td>1918 Index of coincidence</td>
<td></td>
</tr>
<tr>
<td>1918 William Friedman</td>
<td>Kasiski’s method</td>
</tr>
<tr>
<td>1926 Vernam cipher (one-time pad)</td>
<td>Kasiski’s method</td>
</tr>
<tr>
<td>1996 (2nd ed)</td>
<td>1999</td>
</tr>
</tbody>
</table>
Substitution Ciphers (1)

1. Monalphabetic (simple) substitution cipher

\[ M = m_1 m_2 m_3 \ldots m_n \]
\[ C = f(m_1) f(m_2) f(m_3) \ldots f(m_n) \]

Generally \( f \) is a random permutation, e.g.,

\[ f = [a b d e f g h i k l n o p q r s t u v w x y z] \]
\[ f = [a l t a v n c e r u b q p d f k h w y g x z j n i o] \]

Key = \( f \)

Number of keys = \( 26! \approx 4 \cdot 10^{26} \)

Coding characters into numbers

<table>
<thead>
<tr>
<th>Character</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
</tr>
<tr>
<td>F</td>
<td>5</td>
</tr>
<tr>
<td>G</td>
<td>6</td>
</tr>
<tr>
<td>H</td>
<td>7</td>
</tr>
<tr>
<td>I</td>
<td>8</td>
</tr>
<tr>
<td>J</td>
<td>9</td>
</tr>
<tr>
<td>K</td>
<td>10</td>
</tr>
<tr>
<td>L</td>
<td>11</td>
</tr>
<tr>
<td>M</td>
<td>12</td>
</tr>
<tr>
<td>N</td>
<td>13</td>
</tr>
<tr>
<td>O</td>
<td>14</td>
</tr>
<tr>
<td>P</td>
<td>15</td>
</tr>
<tr>
<td>Q</td>
<td>16</td>
</tr>
<tr>
<td>R</td>
<td>17</td>
</tr>
<tr>
<td>S</td>
<td>18</td>
</tr>
<tr>
<td>T</td>
<td>19</td>
</tr>
<tr>
<td>U</td>
<td>20</td>
</tr>
<tr>
<td>V</td>
<td>21</td>
</tr>
<tr>
<td>W</td>
<td>22</td>
</tr>
<tr>
<td>X</td>
<td>23</td>
</tr>
<tr>
<td>Y</td>
<td>24</td>
</tr>
<tr>
<td>Z</td>
<td>25</td>
</tr>
</tbody>
</table>

Monalphabetic substitution ciphers

Simplifications (1)

A. Caesar Cipher

\[ c_i = f(m_i) = m_i + 3 \mod 26 \]
\[ m_i = f^{-1}(c_i) = c_i - 3 \mod 26 \]
No key

B. Shift Cipher

\[ c_i = f(m_i) = m_i + k \mod 26 \]
\[ m_i = f^{-1}(c_i) = c_i - k \mod 26 \]

Key = \( k \)

Number of keys = 26

Caesar Cipher: Example

Plaintext: I C A M E I S A W I C O N Q U E R E D

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>2</td>
<td>0</td>
<td>12</td>
<td>4</td>
<td>8</td>
<td>18</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>14</td>
<td>13</td>
<td>16</td>
<td>20</td>
<td>4</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>7</td>
<td>11</td>
<td>21</td>
<td>3 25</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>17</td>
<td>16</td>
<td>19</td>
<td>23</td>
<td>7</td>
<td>20</td>
<td>7 6</td>
</tr>
</tbody>
</table>

Ciphertext: L F D P H L V D Z L F R Q T X H U H G

Monalphabetic substitution ciphers

Simplifications (2)

C. Affine Cipher

\[ c_i = f(m_i) = k_1 \cdot m_i + k_2 \mod 26 \]
\[ \gcd(k_1, 26) = 1 \]

\[ m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \mod 26 \]

Key = \( (k_1, k_2) \)

Number of keys = \( 12 \cdot 26 = 312 \)
Most frequent single letters

*Average frequency in a random string of letters:*
\[
\frac{1}{26} = 0.038 = 3.8\%
\]

*Average frequency in a long English text:*

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>13%</td>
</tr>
<tr>
<td>T, N, R, I, O, A, S</td>
<td>6%-9%</td>
</tr>
<tr>
<td>D, H, L</td>
<td>3.5%-4.5%</td>
</tr>
<tr>
<td>C, F, P, U, M, Y, G, W, V</td>
<td>1.5%-3%</td>
</tr>
<tr>
<td>B, X, K, Q, J, Z</td>
<td>&lt; 1%</td>
</tr>
</tbody>
</table>

Average frequency in a random string of letters:

1/26 = 0.038 = 3.8%

Digrams:

TH, HE, IN, ER, RE, AN, ON, EN, AT

Trigrams:

THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Relative frequency of letters in a long English text

by Stallings

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in a long English plaintext

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in the corresponding ciphertext for a shift cipher

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in a long English plaintext

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in the corresponding ciphertext for a general monoalphabetic substitution cipher

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Frequency analysis attack: relevant frequencies

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in the ciphertext of the long English text T

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>

Character frequency in the ciphertext of the short English message M

<table>
<thead>
<tr>
<th>Character</th>
<th>Frequency</th>
</tr>
</thead>
</table>
Frequency analysis attack (1)

Step 1: Establishing the relative frequency of letters in the ciphertext

Ciphertext:
FMXVE DKAPH FERBN DKRXR SREFM ORUDS DDKVS HVUFE DKAPR KDLYE VLRHH RH

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>8</td>
</tr>
<tr>
<td>D</td>
<td>7</td>
</tr>
<tr>
<td>E, H, K</td>
<td>5</td>
</tr>
</tbody>
</table>

Frequency analysis attack (2)

Step 2: Assuming the relative frequency of letters in the corresponding message, and deriving the corresponding equations

Assumption: Most frequent letters in the message: E and T

Corresponding equations:
E → R
T → D
4 → 17
19 → 3
f(4) = 17
f(19) = 3

Frequency analysis attack (3)

Step 3: Verifying the assumption for the case of affine cipher

\[ 4 \cdot k_1 + k_2 = 17 \pmod{26} \]
\[ 19 \cdot k_1 + k_2 = 3 \pmod{26} \]
\[ 15 \cdot k_1 = -14 \pmod{26} \]
\[ 15 \cdot k_1 = 12 \pmod{26} \]

Substitution Ciphers (2)

2. Polyalphabetic substitution cipher

\[ M = m_1 \ m_2 \ldots \ m_d \]
\[ m_{d+1} \ m_{d+2} \ldots \ m_{2d} \]
\[ m_{2d+1} \ m_{2d+2} \ldots \ m_{3d} \]

\[ C = f_1(m_1) \ f_2(m_2) \ldots \ f_d(m_d) \]
\[ f_1(m_{d+1}) \ f_2(m_{d+2}) \ldots \ f_d(m_{2d}) \]
\[ f_1(m_{2d+1}) \ f_2(m_{2d+2}) \ldots \ f_d(m_{3d}) \]

\[ d \text{ is a period of the cipher} \]

Key = d, f_1, f_2, ..., f_d

Number of keys for a given period d = (26!)^d = (4 \cdot 10^{26})^d

Polyalphabetic substitution ciphers
Simplifications (1)

A. Vigenère cipher: polyalphabetic shift cipher

Invented in 1568

\[ c_i = f_i_{\text{mod } d}(m_i) = m_i + k_{i \text{mod } d} \pmod{26} \]

\[ m_i = f_i_{\text{mod } d}^{-1}(c_i) = m_i - k_{i \text{mod } d} \pmod{26} \]

Key = k_0, k_1, ..., k_{d-1}

Number of keys for a given period d = (26)^d
Vigenère Square

Vigenère Cipher - Example

Plaintext: TO BE OR NOT TO BE
Key: NSA
Encryption:

TOB
EOR
NOT
TOBE

Ciphertext: GGBRAGTGGBR

Determining the period of the polyalphabetic cipher

Kasiski’s method

Ciphertext: GGBRAGTGGBR

Distance = 9

Period d is a divisor of the distance between identical blocks of the ciphertext

In our example: d = 3 or 9

Index of coincidence method (1)

n_i - number of occurrences of the letter i in the ciphertext

i = a .. z

N - length of the ciphertext

p_i = frequency of the letter i for a long ciphertext

\[ p_i = \lim_{N \to \infty} \frac{n_i}{N} \]

\[ \sum_{i=a}^{z} p_i = 1 \]

Index of coincidence method (2)

Measure of roughness:

\[ M.R. = \sum_{i=a}^{z} \left( p_i - \frac{1}{26} \right)^2 = \sum_{i=a}^{z} p_i^2 - \frac{1}{26} \]

M.R. 0.028 0.014 0.006 0.003
period 1 2 5 10

Index of coincidence method (3)

Index of coincidence

The approximation of \[ \sum_{i=a}^{z} p_i \]

Definition:

Probability that two random elements of the ciphertext are identical

Formula:

\[ I.C. = \sum_{i=a}^{z} \binom{n_i}{2} \binom{N}{2} = \sum_{i=a}^{z} \frac{(n_i-1) \cdot n_i}{(N-1) \cdot N} \]
Index of coincidence method (4)

Measure of roughness

\[ M.R. = I.C. - \frac{1}{26} \sum_{i=1}^{26} (n_i - 1) \cdot n_i = \frac{1}{(N-1) \cdot N} - \frac{1}{26} \]

M.R. 0.028 0.014 0.006 0.003

period 1 2 5 10

Polyalphabetic substitution ciphers
Simplifications (2)

B. Rotor machines used before and during the WWII

<table>
<thead>
<tr>
<th>Country</th>
<th>Machine</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>Enigma</td>
<td>d=26\cdot25\cdot26 = 16,900</td>
</tr>
<tr>
<td>U.S.A.</td>
<td>M-325, Hagelin M-209</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>“Purple”</td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>Typex</td>
<td>d=26\cdot(26-k)\cdot26, k=5, 7, 9</td>
</tr>
<tr>
<td>Poland</td>
<td>Lacida</td>
<td>d=24\cdot31\cdot35 = 26,040</td>
</tr>
</tbody>
</table>

Military Enigma

Enigma Daily Keys

Order of rotors (Walzenlage)

6 combinations
Positions of rings (Ringstellung)

26^3 combinations

Plugboard Connections (Steckerverbindung)

≈ 0.5 \cdot 10^{15} combinations

Initial Positions of Rotors (Grundstellung)

26^3 combinations

Number of possible internal connections of Enigma

3 \cdot 10^{14}

Estimated number of atoms in the universe

10^{80}

Total Number of Keys

3.6 \cdot 10^{22} \approx 2^{75}

Larger number of keys than DES.

Broken by Polish Cryptologists 1932-1940

Marian Rejewski (born 1905)
Jerzy Różycki (born 1909)
Henryk Zygalski (born 1907)
Jul 25-26, 1939: A secret meeting takes place in the Kabackie Woods near the town Pyry (South of Warsaw), where the Poles hand over to the French and British Intelligence Service their complete solution to the German Enigma cipher, and two replicas of the Enigma machine.

Improvements and new methods developed by British cryptologists 1939-1945

Alan Turing (born 1912)
Gordon Welchman (born 1906)

Enigma Timetable: 1939

1939-1940:
Alan Turing develops an idea of the British cryptological "Bombe" based on the known-plaintext attack.

Gordon Welchman develops an improvement to the Turing's idea called "diagonal board".

Harold "Doc" Keen, engineer at British Tabulating Machines (BTM) becomes responsible for implementing British "Bombe".

Enigma Timetable: 1939-1940

May, 1940:
First British cryptological bombe developed to reconstruct daily keys goes into operation.

Over 210 Bombes are used in England throughout the war.
Each bombe weighed one ton, and was 6.5 feet high, 7 feet long, 2 feet wide.

Machines were operated by members of the Women's Royal Naval Service, "Wrens".
Enigma Timetable: 1943

Apr, 1943:
The production of the American Bombe starts in the National Cash Register Company (NCR) in Dayton, Ohio. The engineering design of the bombe comes from Joseph Desch.

Substitution Ciphers (3)

3. Running-key cipher

\[ M = m_1 \ m_2 \ m_3 \dots \ m_N \]
\[ K = k_1 \ k_2 \ k_3 \dots \ k_N \]

\[ K \text{ is a fragment of a book} \]
\[ C = c_1 \ c_2 \ c_3 \dots \ c_N \]
\[ c_i = m_i + k_i \mod 26 \]
\[ m_i = c_i - k_i \mod 26 \]


Substitution Ciphers (4)

4. Polygram substitution cipher

\[ M = m_1 \ m_2 \dots \ m_{d-1} \ m_d = M_1 \]
\[ m_{d+1} \ m_{d+2} \dots \ m_{2d} = M_2 \]
\[ m_{2d+1} \ m_{2d+2} \dots \ m_{3d} = M_3 \]

\[ C = c_1 \ c_2 \dots \ c_{d-1} \ c_d = C_1 \]
\[ c_{d+1} \ c_{d+2} \dots \ c_{2d} = C_2 \]
\[ c_{2d+1} \ c_{2d+2} \dots \ c_{3d} = C_3 \]

\[ d \text{ is the length of a message block} \]
\[ C_i = f(M_i) \]
\[ M_i = f^{-1}(C_i) \]

Key = \( d, f \)

Number of keys for a given block length \( d = (26^d)! \)

Playfair Cipher

Key:

PLAYFAIR IS A DIGRAM CIPHER

```
<table>
<thead>
<tr>
<th>P</th>
<th>L</th>
<th>A</th>
<th>Y</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>R</td>
<td>S</td>
<td>D</td>
<td>G</td>
</tr>
<tr>
<td>M</td>
<td>C</td>
<td>H</td>
<td>E</td>
<td>B</td>
</tr>
<tr>
<td>K</td>
<td>N</td>
<td>O</td>
<td>Q</td>
<td>T</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Z</td>
</tr>
</tbody>
</table>
```

```
Convention 1 (Stallings)
message    POLAND     ciphertext     KAYQR
```

```
Convention 2 (Handbook)
message    POLAND     ciphertext     KAYQR
```

Hill Cipher

1929

Ciphering:

\[ C_{[1\times d]} = M_{[1\times d]} \cdot K_{[d\times d]} \]

\[ (c_1, c_2, \ldots, c_d) = (m_1, m_2, \ldots, m_d) \begin{bmatrix} k_{11}, k_{12}, \ldots, k_{1d} \\ k_{d1}, k_{d2}, \ldots, k_{dd} \end{bmatrix} \]

cipher block = message block \cdot key matrix
**Hill Cipher**

**Deciphering:**

\[ M_{[dxd]} = C_{[dxd]} \cdot K^{-1}_{[dxd]} \]

message block = ciphertext block \* inverse key matrix

where

\[ K_{[dxd]} \cdot K^{-1}_{[dxd]} = \begin{pmatrix} 1, 0, \ldots, 0, 0 \\ 0, 1, \ldots, 0, 0 \\ \vdots \end{pmatrix} \]

\[ = \begin{pmatrix} 0, 0, \ldots, 1, 0 \\ 0, 0, \ldots, 0, 1 \end{pmatrix} \]

key matrix \* inverse key matrix = identity matrix

**Hill Cipher - Known Plaintext Attack (1)**

*Known:*

\[ C_1 = (c_{11}, c_{12}, \ldots, c_{1d}) \quad M_1 = (m_{11}, m_{12}, \ldots, m_{1d}) \]

\[ C_2 = (c_{21}, c_{22}, \ldots, c_{2d}) \quad M_2 = (m_{21}, m_{22}, \ldots, m_{2d}) \]

\[ \ldots \]

\[ C_d = (c_{d1}, c_{d2}, \ldots, c_{dd}) \quad M_d = (m_{d1}, m_{d2}, \ldots, m_{dd}) \]

**We know that:**

\[ (c_{11}, c_{12}, \ldots, c_{1d}) = (m_{11}, m_{12}, \ldots, m_{1d}) \cdot K_{[dxd]} \]

\[ (c_{21}, c_{22}, \ldots, c_{2d}) = (m_{21}, m_{22}, \ldots, m_{2d}) \cdot K_{[dxd]} \]

\[ \ldots \]

\[ (c_{d1}, c_{d2}, \ldots, c_{dd}) = (m_{d1}, m_{d2}, \ldots, m_{dd}) \cdot K_{[dxd]} \]

**Hill Cipher - Known Plaintext Attack (2)**

\[ C_{[dxd]} = M_{[dxd]} \cdot K_{[dxd]} \]

\[ K_{[dxd]} = M^{-1}_{[dxd]} \cdot C_{[dxd]} \]

**Substitution Ciphers (5)**

4. Homophonic substitution cipher

\[ M = \{ A, B, C, \ldots, Z \} \]

\[ C = \{ 0, 1, 2, 3, \ldots, 99 \} \]

\[ c_i = f(m_i, \text{random number}) \]

\[ m_i = f^{-1}(c_i) \]

\[ f: \begin{cases} E &\rightarrow 17, 19, 27, 48, 64 \\ A &\rightarrow 8, 20, 25, 49 \\ U &\rightarrow 45, 68, 91 \\ \ldots \ldots \\ X &\rightarrow 33 \end{cases} \]

**Transposition ciphers**

\[ M = m_1 \ m_2 \ m_3 \ \ldots \ m_N \]

\[ C = m_{(1)} \ m_{(2)} \ m_{(3)} \ \ldots \ m_{(N)} \]

Letters of the plaintext are rearranged without changing them

**Character frequency in a long English plaintext**

**Character frequency in the corresponding ciphertext for a transposition cipher**
### Transposition cipher

**Example**

Plaintext: CRYPTOANALYST

Key: K R I S

Encryption:

<table>
<thead>
<tr>
<th>2 3 1 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>K R I S</td>
</tr>
<tr>
<td>C R Y P</td>
</tr>
<tr>
<td>T A N A</td>
</tr>
<tr>
<td>L Y S T</td>
</tr>
</tbody>
</table>

Ciphertext: YNSCTLRAYPAT

### One-time Pad

**Vernam Cipher**

Gilbert Vernam, AT&T

Major Joseph Mauborgne

1926

\[ c_i = m_i \oplus k_i \]

<table>
<thead>
<tr>
<th>m_i</th>
<th>011101101010101011101101</th>
</tr>
</thead>
<tbody>
<tr>
<td>k_i</td>
<td>11011101110110111101101</td>
</tr>
<tr>
<td>c_i</td>
<td>101010110111111100011</td>
</tr>
</tbody>
</table>

All bits of the key must be chosen at random and never reused

### Perfect Cipher

Claude Shannon

Communication Theory of Secrecy Systems, 1948

\[ \forall m \in M, \quad P(M=m | C=c) = P(M=m) \]

\[ m \in M, \quad c \in C \]

The cryptanalyst can guess a message with the same probability without knowing a ciphertext as with the knowledge of the ciphertext

### Is substitution cipher a perfect cipher?

\[ C = XRZ \]

\[ P(M=ADD | C=XRZ) = 0 \]

\[ P(M=ADD) \neq 0 \]

\[ M = \text{CAT, PET, SET, ADD, BBC, AAA, HOT, HIS, HER, BET, WAS, NOW, etc.} \]

### Is one-time pad a perfect cipher?

\[ C = XRZ \]

\[ P(M=ADD | C=XRZ) \neq 0 \]

\[ P(M=ADD) \neq 0 \]
S-P Networks

Basic operations of S-P networks

Substitution
Permutation

\[
\begin{array}{cccc}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
\end{array}
\]

S-box
P-box

Avalanche effect

Shannon Product Ciphers

- Computationally secure ciphers based on the idea of diffusion and confusion
- Confusion relationship between plaintext and ciphertext is obscured, e.g. through the use of substitutions
- Diffusion spreading influence of one plaintext letter to many ciphertext letters, e.g. through the use of permutations

LUCIFER

LUCIFER- external look

16 rounds

128 bits
512 bits
128 bits