Introduction To Cryptography

History & Basics

A Very Brief History

Atbash

500-600BC  ATBASH Cipher (reverse alphabet)

Aleph Bet  Yod Kaph
ך ... ז
ל ... ש

Area

Babel -> Sheshach

Aleph Bet  Yod Kaph
ך ... ז
ל ... ש

Taw Shin  Mem Lamed
Skytale
487 BC  Skytale or scytale (σκυτάλε)

Polybius’ Cipher

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>2</td>
<td>f</td>
<td>g</td>
<td>h</td>
<td>ij</td>
</tr>
<tr>
<td>3</td>
<td>l</td>
<td>m</td>
<td>n</td>
<td>o</td>
</tr>
<tr>
<td>4</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
</tr>
<tr>
<td>5</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
</tr>
</tbody>
</table>

- 200 BC
- used with torches in antiquity
- Bipartite substitution cipher
- Prisoner’s Cipher (see Koestler’s Darkness at Noon)
- Nihilist cipher based on it

Substitution and Transposition

Two basic methods of encryption

Substitution

- Replace letter/symbol/text with other letter/symbol/text
- leads to confusion

Transposition

- Rearrange the order of letters/symbols in the text
- leads to diffusion
Caesar’s Cipher

40-50BC Caesar Cipher (Substitution Cipher)

omnia gallia est divisa in partes tres
RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

• First cipher documented in military use.
• Generalization (with shift other than 3, also sometimes, inaccurately, called Caesar Cipher)

Al-Kindi (801-873)

“A Manuscript on Deciphering Cryptographic Messages”

• cryptanalytic methods
  • cribs
  • vowel-consonant combinations
• frequency analysis
• classification of ciphers
• linguistic analysis (letter frequencies)

Taken from Al-Kadi, Origins of Cryptology-The Arab Contribution, Cryptologia, 2, 2010

Al-Kindi and Frequency Analysis

One way to solve an encrypted message if we know its language, is to find a text of the same language long enough … and then count each letter of it. We call the most frequently occurring letter the “first”, … and so on. Then we look at the cryptogram we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the “first” letter.

Taken from Al-Kadi, Origins of Cryptology-The Arab Contribution, Cryptologia, 2, 2010
**Al-Kindi’s Classification**

Taken from Al-Kadi, *Origins of Cryptology: The Arab Contribution*, Cryptologia, 2, 2010

---

**Alberti’s Cipher Disk**

Invented by Leon Battista Alberti in 1460s.

Correspondents agree on index letter on inner disk. Key: corresponding letter on outer disk. Key can change during encryption

---

**Johannes Trithemius**

1462-1516, Germany

*Polygraphiae, 1518*

First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key

*Steganographia, 1606*

- hidden writing
Polygraphiae I
Ave Maria Cipher

Polygraphiae II
Tabula recta, from the 6th book of the Polygraphiae.

- Polyalphabetic substitution
- Progressive key

Examples
- SUGKESUOAKATXO
- QUWWWQSGQSDZ

Bacon’s Bilingual cipher I
1561-1626, England

First idea: encode letters in binary (1623)
Bacon’s Biliteral cipher II

Wisdom and understanding are more to be desired than riches.

Second idea: use two different typefaces to encode a/b decision.

Example: tobeOrnottoBeThaTISThE

Question

Blaise de Vigenère

Traité de Chiffres, 1585

Autokeys:

<table>
<thead>
<tr>
<th>key</th>
<th>plain</th>
<th>cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA UNO MD ELETNE</td>
<td>au nom de l’eternal</td>
<td>XI AHG UP TMLSHXT</td>
</tr>
<tr>
<td>DX HEE CO UMKGNABQ</td>
<td>au nom de l’eternal</td>
<td>XH EEC OU MXGNABQO</td>
</tr>
</tbody>
</table>

Vigenère Cipher

Thomas Jefferson

Wheel cipher (1790s)

- Polyalphabetic
- Mixed alphabets
- Key determines sequence of wheels

Reinvented by Parker Hitt (1913) and used by the military (M-138-A of WW-II)

http://members.aon.at/cipherclerk/VirtualM94.html
ADFGX and ADFGVX

• Invented by Fritz Nebel (1891-1967)
• Combination of digraphic substitution (like Polybius) and columnar transposition (based on keyword)
• Introduced by German intelligence as ADFGX in 1918 as a field cipher.
• Later, a sixth letter, V, was added: ADFGVX
• Fractional system

Lester S. Hill

Cryptography in an Algebraic Alphabet, 1929

• Block substitution cipher
• Based on matrix algebra

Enigma

• Rotor machine, 1923; similar machines invented, and patented, earlier, by Koch (Netherlands), Damh (Sweden), and Hebern (US)
• Used by Germans in WWII
• First broken by Rejewski (Poland), then in Bletchley Park by Turing and others.

http://www.enigmaco.de/
Rotors

Wired inside to implement a (fixed) permutation.

Feistel Ciphers

• Type of block ciphers invented by Horst Feistel at IBM Watson Research labs in 60s. Works in binary, and is based on repeated substitution, transposition.

• Lucifer

• With modifications to S-boxes (substitution part), Lucifer is adopted as DES (Data Encryption Standard) by US government in 1976
Diffie, Hellman, Merkle

New Directions in Cryptography, 1976

• First publication of public key cryptography in open literature

• Describes method allowing two parties to agree on a secret key using public channels

RSA

Rivest, Shamir, Adleman, 1977 find a mathematical way of implementing public-key cryptography: RSA.

Both Diffie/Hellman key exchange, and RSA was discovered earlier by British intelligence, but not published (or patented).

Quantum Cryptography

Charles Bennett, Gilles Brassard, 1990 develop quantum cryptography, using quantum physics to secure a channel.
AES

In 2001 Rijndael is adopted as AES (Advanced Encryption Standard), replacing DES as the accepted government standard for secure communication.

Basic Notions

Cryptology

Cryptography:
secret writing (κρυπτος hidden)

Cryptanalysis:
breaking codes and ciphers
Codes and Ciphers

Codes and ciphers render a plaintext message unintelligible by applying transformations to the plaintext (encoding, or enciphering the text).

*Code:* the basic transformation is substitution by codewords.

*Cipher:* the basic transformation is substitution of letters/symbols by letters/symbols.

*Cipher* is often used to denote arbitrary encryption schemes.

Steganography and Cryptography

στήγανος: covered

γράφων: (to) write

κρυπτός: hidden

Steganography tries to hide the presence of message.

Cryptography tries to obscure the contents of the message.

Steganography

message on silk in wax balls
(ancient China)

Xerxes (Herodotus)
invisible inks (at least 100AD)
hollow heels
microdots
IP timing delays
(covert channels)
Coding Theory

- noisy channel
- plaintext encode → codewords → decode → plaintext

Error-Correcting Code: guard against noisy channel

Secret Communication

- Alice plaintext encrypt → ciphertext decrypt → Bob plaintext
- Encryption Key → open channel → Eve → Decryption Key

Keys

Encryption and decryption can depend on a key which is kept secret.

The collection of possible keys is called the key space.

If we assume that only the key, not the method of encryption is secret, the combinatorial complexity, that is, the size of the key space is a first rough measure of how hard it is to break a cipher.
Eve’s Goals

• Reading secret messages — Oscar
• Finding key
• Corrupting messages (Integrity) — Mallory
• Masquerade as Alice (Authentication)

Types of Attack

• Ciphertext only
• Known plaintext (cribs)
• Chosen plaintext
• Chosen ciphertext

Kerckhoff’s Principle

Compromise of the system should not inconvenience the correspondents.

Auguste Kerckhoff
La Cryptographie Militaire, 1883