25/0 /2025

S 6160 ryptology Lectu lassical iphers and Per Secrecy

Maria Francis

ugust 25, 2025

aeser ipher/Shift ipher

Named after Julius Ceaser who used it to commu
his generals.

Replace each letter with one that is a fixed numb
down the alphabet.

Ceasar cipher

$$\mathcal{M} = \{\ \ , B, \ldots, Z\}^*$$

$$\mathcal{K} = \{0, 1, 2, \ldots, 25\}$$

$$Gen = k, k \in \mathcal{K}$$

$$Enc_k(m_1 m_2 \ldots m_n) = (c_1 c_2 \ldots c_n),\ \text{where } c_i = m_i +$$

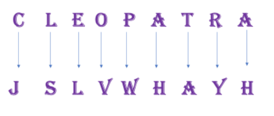
$$Dec_k(c_1 c_2 \ldots c_n) = (m_1 m_2 \ldots m_n) \text{ where } m_i = c_i$$

25/0 /2025

aeser ipher/Shift ipher

Encrypted messages look scrambled (unless k is

Encrypt with $k = 7$



Cryptanalysis

We just need to try all 26 different values of k s
resulting plaintext is readable.

If the message is relatively long, the scheme is e

25/0 /2025

Substitution ipher

Choose a permutation of the alphabet set $\{\ \ ,$ and apply that to all letters in the plaintext.

Permutation : one-one, onto function from a set

Brute-force won't work – you have to try 26 ≈ 2 keys.

Substitution Cipher

$$\mathcal{M} = \{\ \ , B, \ldots, Z\}^*$$

$$\mathcal{K} = \text{the set of permutations of } \{$$

$$Gen = \ \ , \quad \in \mathcal{K}$$

$$Enc\ (m_1 m_2 \ldots m_n) = c_1 c_2 \ldots c_n, \text{ where } c_i = \quad (m_i$$

$$Dec\ (c_1 c_2 \ldots c_n) = m_1 m_2 \ldots m_n \text{ where } m_i =$$

Cryptanalysis of Substitution Cipher ?

25/0 /2025

Different types of attacks

Passive attack – Ciphertext-only attack : ttack
with only ciphertexts. Most difficult attack.

Passive attack – Known-plaintext attack (KP):
given the pair (plaintext, ciphertext). Relevant be
attacker may know side information (e.g: headers
him to deduce some plaintexts.

ctive attack – Chosen-plaintext attack (CP):
obtains (plaintext, ciphertext) where plaintexts ar
choice. e.g: information we encrypt is not guaran
from trusted sources.

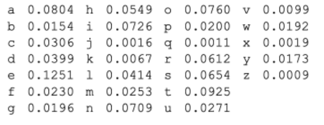
ctive attack – Chosen-ciphertext attack (CC):
requests (plaintext, ciphertext) for arbitrary ciphe
choice. E.g: We cannot always trust the provena
ciphertexts we decrypt.

ryptanalysis of Substitution iph

Chosen plaintext attack - completely insecure!

Ciphertext only (passive) attack? – Frequency an

E.g: in the ciphertext, if x is the most common l
likely that $(e) = x$.



a	0.0804	h	0.0549	o	0.0760	v	0.0099
b	0.0154	i	0.0726	p	0.0200	w	0.0192
c	0.0306	j	0.0016	q	0.0011	x	0.0019
d	0.0399	k	0.0067	r	0.0612	y	0.0173
e	0.1251	l	0.0414	s	0.0654	z	0.0009
f	0.0230	m	0.0253	t	0.0925		
g	0.0196	n	0.0709	u	0.0271		

Probability distributions of 1-grams in English.

dditionally, we need to make use of the frequencies o
(two letter seq.) and trigrams (three letter seq.) in th
language. For e.g. frequent three letter words : "and",

Vigenère cipher

So far, all were monoalphabetic ciphers – each sy
plaintext is mapped to a unique symbol in the cip
on the secret key.

Vigenère cipher is a polyalphabetic cipher – same
symbol can be mapped to more than one ciphert

generalization of the shift cipher where each le
plaintext is shifted by different amounts.

Key is a string $k = k_1 \dots k_n$ with $k_i \in \{0, \dots, 25$

Encryption of $m = m_1 \dots m_l$ under key k is
$(m_1 + k_1 \bmod 26)(m_2 + k_2 \bmod 26) \dots (m_n + k_n \bmod 26)(m_{n\ 1} + k_1 \bmod 26), \dots)$.

Vigenère cipher

$$\mathcal{M} = \{\ \ , B, \dots, Z\}^*$$

$$\mathcal{K} = \{k = (k_1 \dots k_n) : k_i \in \{0, \dots,$$

$$Gen = k, k \in \mathcal{K}$$

$$Enc_k(m_1 m_2 \dots m_l) = c_1 c_2 \dots c_l, \text{ where } c_i = m_i + k$$

$$Dec_k(c_1 c_2 \dots c_l) = m_1 m_2 \dots m_l \text{ where } m_i = c_i$$

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V

ryptanalysis of Vigenère cipher

If both the plaintext and the ciphertext are know
break the system. Just compute the difference be
letter in the ciphertext and the plaintext.

nd insecure of course with a chosen plaintext at

What about ciphertext only attack?

The key space is of size 26^n so except for small n
attack is not possible.

Frequency distribution wont work.

Charles Babbage and "Kasiski Test" (Both came
independently and Babbage was earlier.)

25/0 /2025

‘Kasiski Test”

First step - determining n

Determine the keyword length n.

ny two (or more) identical segments of plaintex to the same ciphertext letters whenever the dista multiple of n.

Look for identical segments of the ciphertext.

Suppose we have m such identical segments.

Record the distance between starting position o say l , $l_2, \ldots$

Prove : n divides l , l_2 and n divides the gcd of therefore n is the G D.

‘Kasiski Test”

nother way to determine n

Guess for n and divide the ciphertext into n bins
$B_0, B_1, \ldots, B_{n\ \ 1}$ by placing the ith ciphertext int

If the frequency distribution of the symbols n eac
resembles the expected distribution of a “meaning
text, then our guess is most probably correct.

25/0 /2025

‘Kasiski Test”

Second step - determining the keyword

- Suppose we have got the correct keyword length ciphertext symbols are arranged in bins $B_0, \ldots, B$ Strategy II.
- The ciphertext symbols in each bean B_i is the res applying a “shift cipher" (i.e., a cyclic shift of the corresponding plaintext letters.)
- Use the frequency distribution of ciphertext symb make a guess for the ith letter of the keyword.
- Use partial guesses for the key letters to guess th

Vernam ipher – One Time Pad

$$\mathcal{M} = \{0,1\}^*$$

$$\mathcal{K} = \{0,1\}^* \text{ where key length = me}$$

$$Gen = k, k \in \mathcal{K}$$

$$Enc_k(m_1 m_2 \dots m_n) = c_1 c_2 \dots c_n, \text{ where } c_i = m_i \oplus k$$

$$Dec_k(c_1 c_2 \dots c_n) = m_1 m_2 \dots m_n \text{ where } m_i = c_i \oplus$$

Vigenère cipher with key length equal to the leng plaintext.

Key must be chosen in a completely random way used once.

Perfectly secret but impractical! Key should be a message and used only once.

One Time Pad

Encrypting and Decrypting : just XOR with the s

$$Enc_k(m) = c = m \oplus k$$
$$Dec_k(c) = m = c \oplus k$$

Why is it secure? Every $m \in \mathcal{M}$ and ciphertext c
correspond to a unique key k

What is perfect secrecy?

method is secure iff the odds of the adversary
m are the same whether or not he has seen c.

How to formalize this notion?

Perfectly Secret Encryption

Definition

Let $m \in \mathcal{M}$ be a random message and $c \in \mathcal{C}$ be the c
m. The encryption scheme is said to be perfectly secu
adversary $Pr[M = m|C = c] = Pr[M = m]$.

One Time Pad is Perfectly Secure

Proof:To show that $Pr[M = m|C = c] = Pr[M = m]$
m, c.

$$Pr[(M = m|C = c)] = \frac{Pr[(M = m \cap C = c)]}{Pr[C = c]}$$

by Bayes law,

$$= \frac{Pr[(M = m)] \cdot Pr[(C = c|M =}{Pr[C = c]}$$

by conditional prob. def.,

$$= \frac{Pr[(M = m)] \cdot Pr[(C = c}{{}_{m \in \mathcal{M}}(Pr[M = m\ ] \cdot Pr[C =}$$

by expanding Pr[C=c] as the sur

Proof ontd

Note that $Pr[C = c|M = m\,] = Pr[k = c \oplus m\,]$

Since every $k \in \{0,1\}^n$ is equally likely to be a k
$Pr[k = c \oplus m\,] = \frac{1}{2^n}$.

$$Pr[M = m|C = c] = \frac{Pr[M = m] \cdot \frac{1}{2}}{_{m\,\in\mathcal{M}}(Pr[M = m}$$

$$= \frac{Pr[M = m]}{_{m\,\in\mathcal{M}}(Pr[M = m}$$

$$= \frac{Pr[M = m]}{1}$$

Shannon’s result

OTPs are not practical especially because of the

Can we have a clever way of getting perfect secre shorter keys? Unfortunately the answer is no!

Theorem (Shannon)

For any perfectly secure scheme where lice and Bob from space $\mathcal{K}$ and can encrypt any message m from sp must have $|\mathcal{K}| \geq |\mathcal{M}|$.

Thus OTP is optimal in this regard. nybody else cla they have discovered an unbreakable cipher with short wrong!

Shannon's result - Proof

For any valid ciphertext c, let be the number o

that could result from the decryption of c.

Let us estimate in two ways:

For a given key $k \in \mathcal{K}$ there can be at most one

could decrypt c in at most one way for each k.

Thus $| \quad | \leq |\mathcal{K}|$.

Claim : $| \quad | = |\mathcal{M}|$, i.e. every $m \in \mathcal{M}$ can result

c.

If not for some m, then $Pr[M = m] > 0$ before w

$Pr[M = m | C = c] = 0$, contradiction to perfect

Thus, $| \quad | = |\mathcal{M}| \leq |\mathcal{K}|$.

25/0 /2025

Observations

Perfect secrecy is w.r.t. computationally unbounc

Is this true? : Every encryption scheme for which $|\mathcal{M}|$ and for which the key is chosen uniformly fr perfectly secret. : False.

Let $\mathcal{M} = \{a, b\}$, $\mathcal{K} = \{k\ , k_2\}$, $\mathcal{C} = \{0, 1\}$.
Let $Enc_k(a) = 0$ and $Enc_k(b) = 1$ for $k = k\ , k_2$
Dec algorithm will return a on input ciphertext
input ciphertext 1.
learly, the scheme is correct.

$$Pr[M = a|C = 1] = 0 \neq (1/2) = Pr[M$$

not perfectly secret!

Gen must choose the key uniformly from the set
that is not enough! for every message m and cip
there is a unique key mapping m to c

Observations/Exercises

Ceaser cipher is definitely not secure. What if we
one letter? i.e., $\mathcal{M} = \mathcal{C} = \{0, \ldots, 25\}$ and not
$\{0, 1, \ldots, 25\}^*$? Prove that in such a scenario it
secure cipher!

Consider an encryption scheme (Gen, Enc, Dec)
two messages $m, m\ \in \mathcal{M}$ the distribution of the
when m is encrypted is identical to the distributio
ciphertext when $m\ $ is encrypted. i.e.

$$Pr[Enc\ \ (m) = c] = Pr[Enc\ \ (m\ ) = c], \forall$$

The encryption scheme is said to have adversaria
indistinguishability .

Q: Show that it is equivalent to saying an encryp
perfectly secret.