Define — secure encryption → create such methods

more security goals

---

9 Jan 25

TIGER → permute no^s = 120

Program — to attack $\boxed{\text{substitution cipher}}$

use (i) plaintext statistics

(ii) dictionary of words

(ii) can be eliminated, and the attack made completely automated.

3rd toy cipher : Vigenére cipher

→ extend shift cipher

Shift cipher

Plaintext	Ciphertext	
a →	a+(x)	← Shift
b →	b+(x)	
⋮		

} easy attack: brute force

plaintext : attack at dawn

Secret word = $\boxed{\text{secret key}}$ = CRY

Encryption:

a t t a c k a t d a w n..

+ C R Y C R Y C R Y C R Y...

ciphertext = c .. .. . . - - - - -

A = 0
B = 1
C = 2
⋮
Z = 25

Cryptanalysis :

$\boxed{\text{Kerckhoff's rule}}$ ← ciphertext is given to you, method is known but key is unknown

La Cryptography Militaire

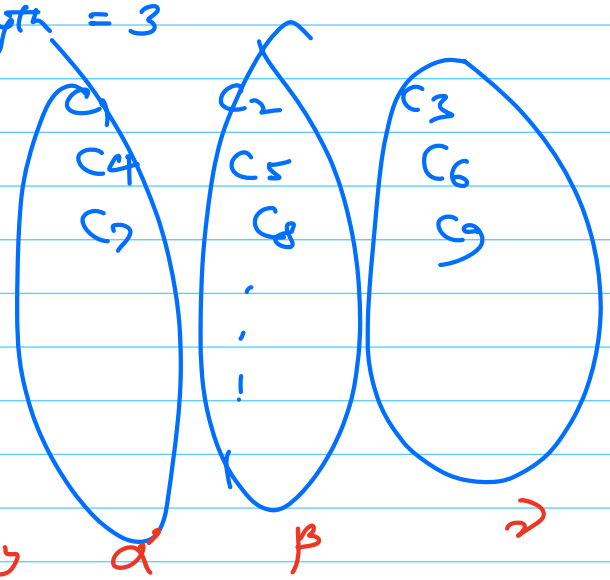
Security by obscurity (i.e hiding the method) ✗

How to attack:

Que: Suppose you knew the key length. Can you attack the system?

Ciphertext: $c_1\, c_2\, c_3\, c_4\, c_5\, c_6\, c_7\, c_8 \ldots\ldots$

(given) key length $= 3$



if prob of ith letter in plaintext $= p_i$

($p_0, p_1, p_2 \ldots p_{25}$ = for English characters) $\longrightarrow$ known

prob of ciphertext letters

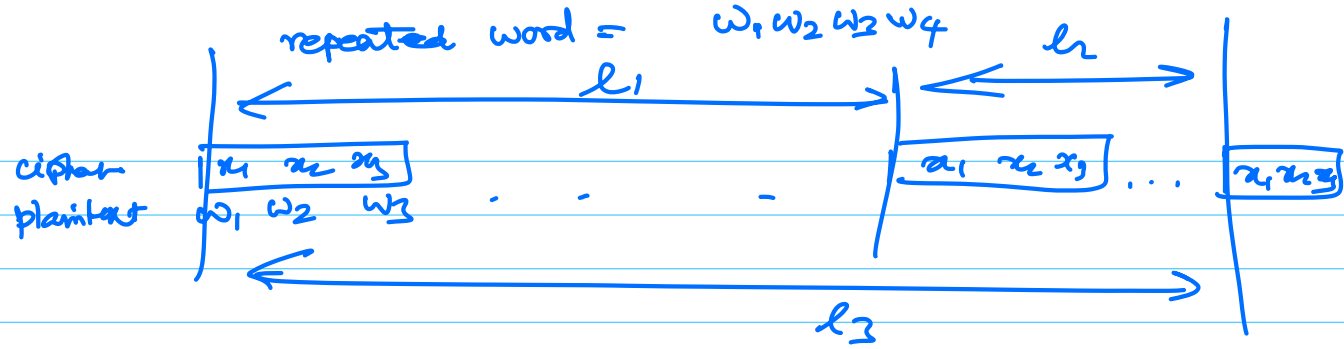
$q_0, q_1, q_2 \ldots q_{25}$

if shift $= \alpha$ then $p_i \simeq q_{i+\alpha}$

Part 2: How to find the length of the key word?

(i) brute force

(ii) Kasiski's test



l_1, l_2, l_3 are all likely to be multiples of key length

$\Rightarrow$ key length $\leq$ gcd(l_1, l_2, l_3)

(iii) Some brute force + some statistical observation

plaintext = $m_1\ m_2\ m_3 \quad m_4\ m_5\ m_6 \quad m_7\ m_8\ m_9 \quad \ldots$

key = + $k_1\ k_2\ k_3 \quad k_1\ k_2\ k_3 \quad k_1\ k_2\ k_3 \quad \ldots$

ciphertext $c_1 \quad c_7$

$c_1\ c_2\ c_3 \quad . \quad . \quad - \quad -$

guess = length = 2	guess = 3	guess = 4
c_1 c_2	c_1 c_2 c_3	c_1 c_2 c_3 c_4
c_3 c_4	c_4 c_5 c_6	c_5 c_6 c_7 c_8
c_5 c_6	c_7 c_8 c_9	⋮
c_7	⋮	

if key length guess = correct

$\rightarrow$ each column represent shuffled English characters

if key length guess = wrong

$\rightarrow$ random shifts

Index of coincidence

- measure of how likely is it that the column is simply shifted alaphets

vs random alphabets

for correct guess

$$\sum p_i^2 = \sum (p_0)^2 + (p_1)^2 + (p_2)^2 + \dots$$

$$= 0.065$$

for any guess

$$\frac{1}{26}(p_0 + p_1 \dots p_{25})$$

$$\simeq \frac{1}{26}$$

$$\simeq 0.038$$

Assignment 1 :

ciphertext 1

↓

Some random text from internet

↓

Encrypted using substitution cipher

- plaintext = { a-z, A-Z, 0-9, ., $, ; ... }
- hidden code word

↓

to be submitted

ciphertext will be different

ciphertext 2

Encrypted by Vigenere cipher

(i) length of the key,

(ii) key word

↓

to be submitted

The Code Book : Simon Singh

What is secure encryption?

① Looking at the ciphertext, no one should be able to find the secret key

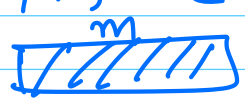
$$Enc(k, m) = m \quad ; \quad Dec(k, c) = c$$

Valid Encryption algorithm:

$$\forall k, \forall m \qquad Dec(k, Enc(k, m)) = m$$

② Looking at the ciphertext, no one should be able find the message

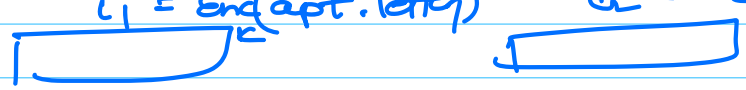
$Enc(k, m) = c$



there exists an algorithm $\mathcal{A}(c) \rightarrow$

③ Looking at the ciphertext, not even a single bit of the plaintext should be revealed

$c_1 = Enc_k(\text{apt. letter}_1)$ $\qquad$ $c_2 = Enc_k(\text{appt. letter}_2)$



c_1, c_2 given

goal: One should not be able to figure out if $m_1 > m_2$ or not.

non-trivial

No efficiently computable function of the message should be revealed by looking at the ciphertext.

<u>plaintext</u>: $\{01, 00\}$

$$Enc(k, \cdot) = c$$

Looking at the ciphertext, $\mathcal{A}$ can predict the following:

"the first bit of the plaintext is 0".

<u>Textbook</u>: Introduction to Modern Cryptography.
Katz & Lindell
CRC Press.

---

10 Jan 25

<u>Recap</u>: What is a <u>secret</u> (secure) encryption?

$\mathcal{P}$ = set of plaintexts = $\{m_1, m_2, \ldots\ldots m_\ell\}$

$\mathcal{C}$ = set of ciphertexts = $\{c_1, c_2, \ldots\ldots c_{\ell'}\}$

(obviously: $\ell' \geq \ell$)

$\mathcal{K}$ = set of keys = $\{k_1, k_2, \ldots k_t\}$