

Cryptography

Hemant Ghayvat

Department of Computer Science and Media Technology

hemant.ghayvat@lnu.se



Motivation!

What do we know about the cyberattack that forced hundreds of Swedish supermarkets to close?

AFP/The Local

news@thelocal.se

@thelocalsweden

6 July 2021

08:55 CEST

Coop

Share this article



A closed Coop store in Stockholm. Photo: Ali Lorestani/TT

Swedish supermarket chain Coop was forced to shut around 800 stores after a major cyberattack which has potentially also hit more than 1,000 companies worldwide.

Hackers are demanding \$70 million in bitcoin in exchange for data stolen in the

CIA !



Outline

Encryption Principles

Encryption (Cipher) Algorithms

Cipher Block Modes of Operation

Key Distribution



Cryptography

Cryptography

Encryption

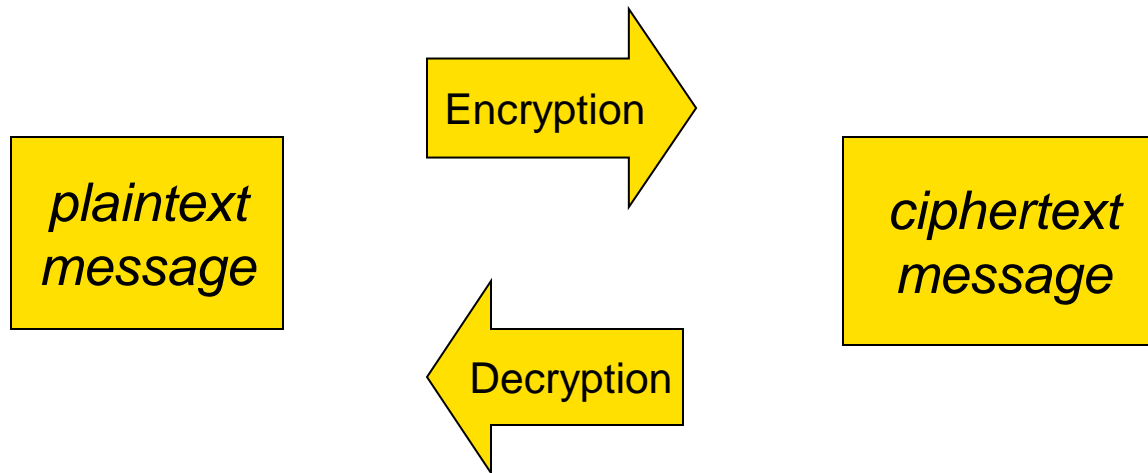
Decryption

Cipher

Key



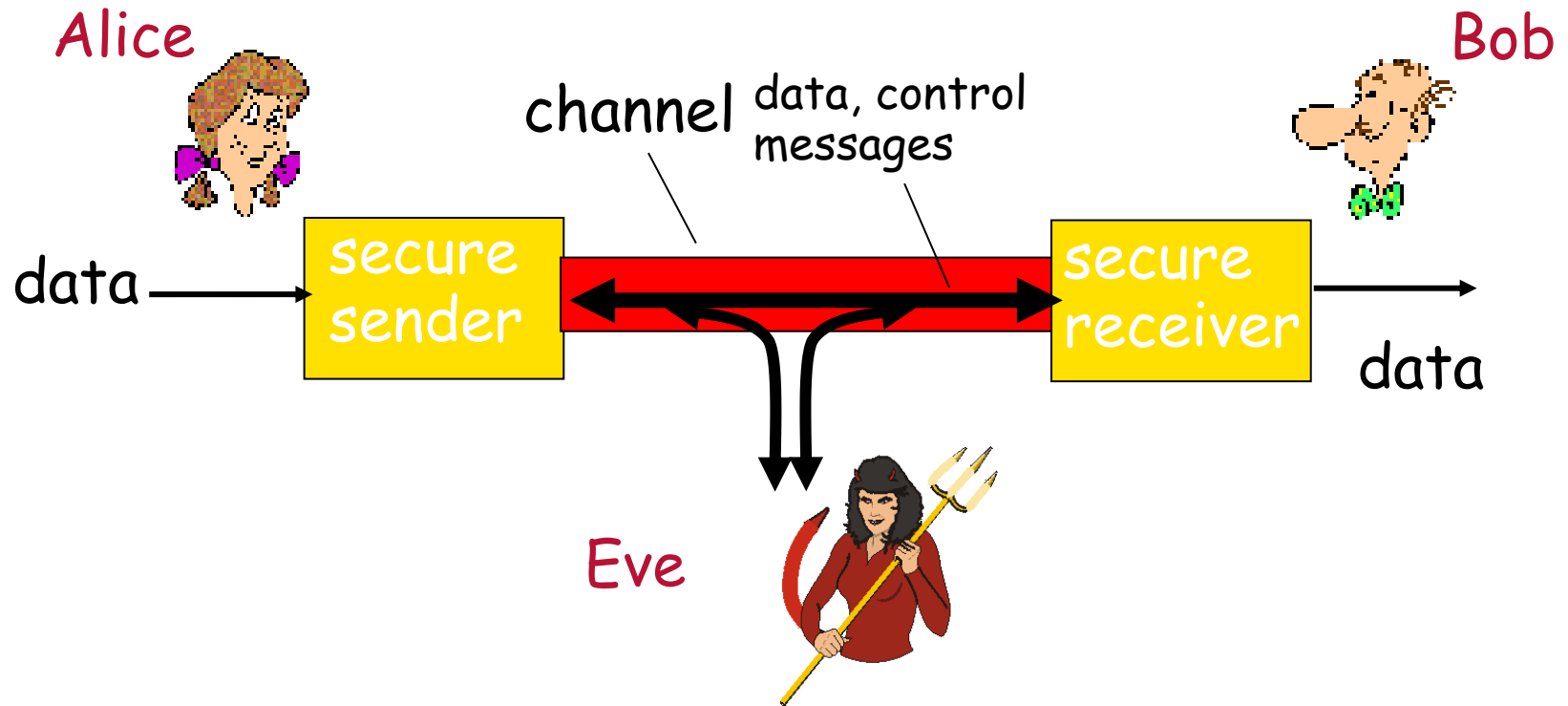
Cryptography



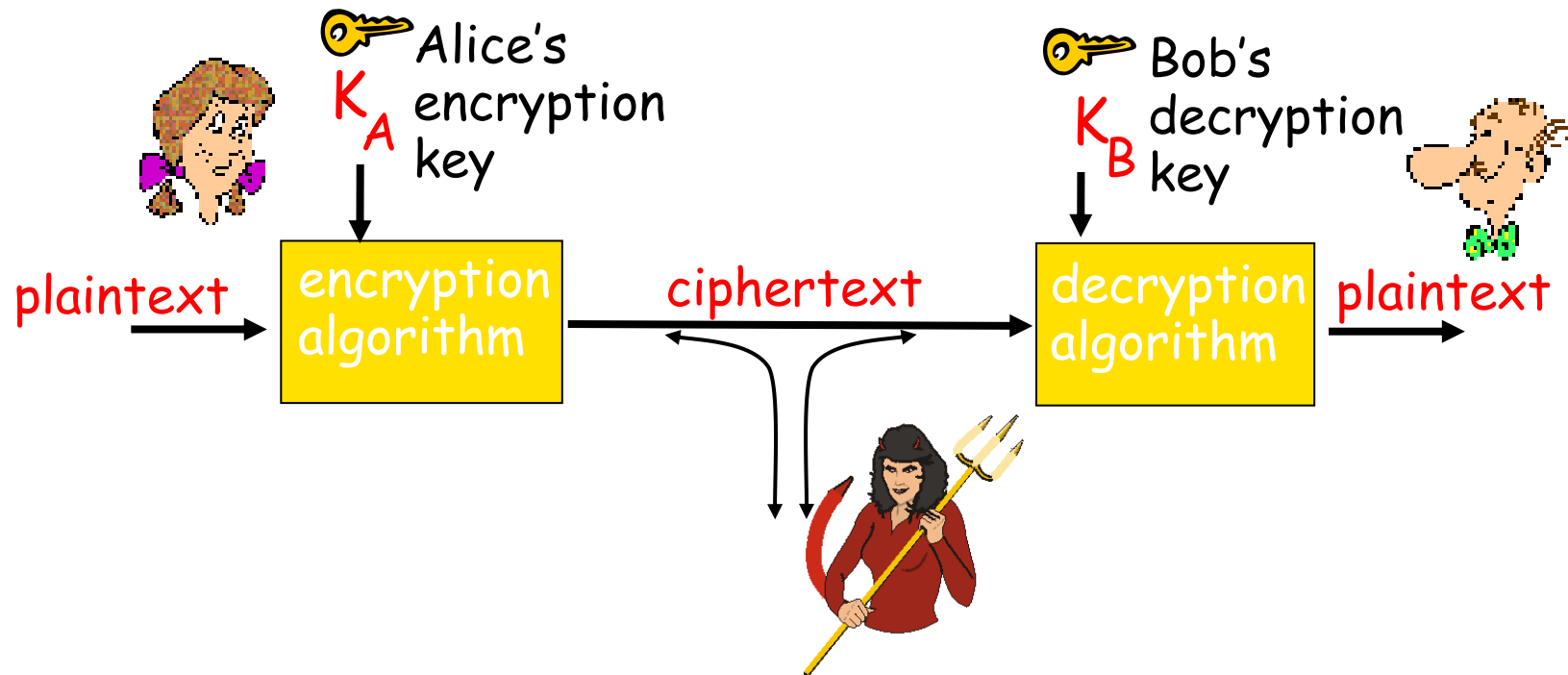
Encrypted(Information) cannot be read

Decrypted(Encrypted(Information)) can be

Friends and enemies: Alice, Bob, Eve



The language of cryptography



symmetric key crypto: sender, receiver keys identical

Cryptanalysis

The process of decrypting a message without knowing the cipher or the key used to encrypt it.

Substitution and transposition ciphers are easy for modern computers to break
To protect information more sophisticated schemes are needed

What is the criteria for the secure encryption algorithm:

1. Cost of breaking is greater than the encrypted information
2. Performing the cryptanalysis would take significant amount of time, sometimes lifetime.



Brute-Force Attack



Classical Cryptography

Substitution Cipher

- Simple substitution cipher (Caesar cipher)
- Monoalphabetic Cipher
- Playfair Cipher
- Polyalphabetic Cipher

Transposition Cipher





Caesar ciphers

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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Substitute the letters in the second row for the letters in the top row to encrypt a message
 - Encrypt(COMPUTER) gives
FRPSXWHU
- Substitute the letters in the first row for the letters in the second row to decrypt a message
 - Decrypt(Encrypt(COMPUTER))
= Decrypt(FRPSXWHU) = COMPUTER



Caesar Cipher

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

P(Plain text) = HELLO WORLD

$K=3$; formula for ciphertext (C)

Encryption:-

$$C = (P+K) \bmod 26$$

Let's begin with H

$$C_H = (7+3) \bmod 26 \Rightarrow 10 \bmod 26$$

↑ weight value from above

$C_H \Rightarrow 10$ [we didn't perform modulus operation as remainder would be in decimal point]

$$C_H = K$$

Similarly P \Rightarrow HELLO WORLD
 $\downarrow \downarrow \downarrow \downarrow \downarrow$
 C \Rightarrow KHOOR

Decryption

$$P = (C-K) \bmod 26$$

$$P_K = (10-3) \bmod 26 \Rightarrow 7 \bmod 26 \Rightarrow 7$$

$$P_K = H$$

Let's take some more examples

Plaintext (P) = XYZ

$$C_Y = (24+3) \bmod 26 \\ = 27 \bmod 26 \\ = 1 \Rightarrow B$$

$$C_X = (23+3) \bmod 26 \\ = 26 \bmod 26 \Rightarrow 0 \Rightarrow A$$

$$C_Z = (25+3) \bmod 26 \Rightarrow 28 \bmod 26 \\ \Rightarrow 2 \Rightarrow C$$

$$C_{(XYZ)} \Rightarrow ABC$$

Now let's calculate plaintext (Decryption)

$$P_A = (C-K) \bmod 26 \Rightarrow (0-3) \bmod 26 \\ \Rightarrow -3 \bmod 26$$

[In mod negative not allowed]

$$\Rightarrow (26-3) \bmod 26 \Rightarrow 23 \bmod 26 \\ \Rightarrow 23 \Rightarrow X$$



Brute Force Crypto Analysis of the Caesar Ciphers

- Brute-force cryptanalysis
 - Simply try all the 25 possible keys

- Three issues with Caesar that make it vulnerable against the brute force:
 1. The encryption/decryption algorithm are known
 2. There are only 25 keys to try
 3. The language of the plaintext is known and easily recognized



Monoalphabetic Cipher

- Rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random cipher text letter hence key is 26 letters long (26! (permutation combination))

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA



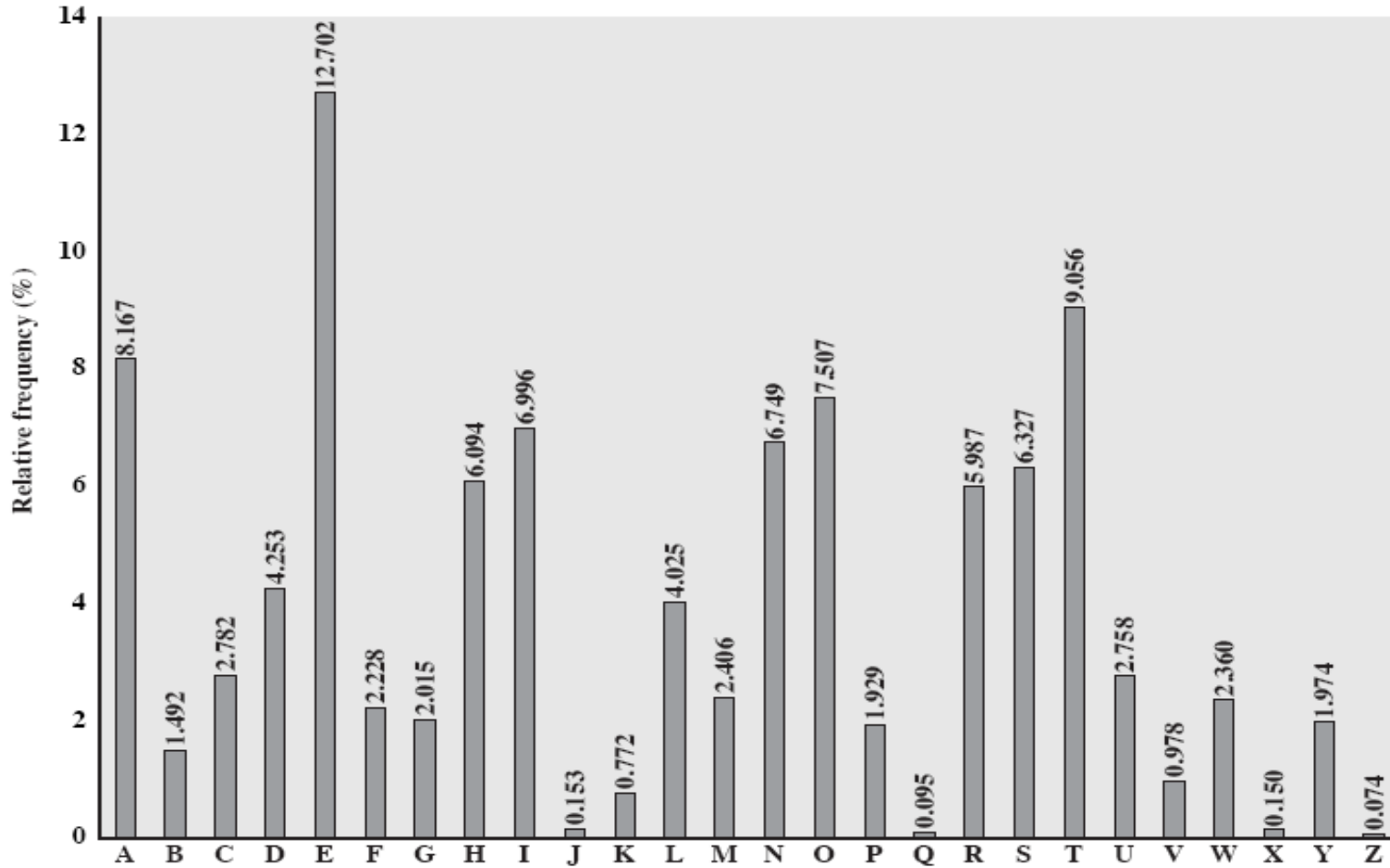
Monoalphabetic Cipher Security

With so many keys, might think the system is secure



But would be **!!!WRONG!!!**

English Letter Frequencies



Polyalphabetic Cipher

- Instead of having one key (table) that is used to encrypt each block of plaintext, we use several different keys.
- The Vigenère cipher is the classical example.



Vigenere Cipher

- Idea: Uses Caesar's cipher with various shifts, in order to hide the distribution of the letters.
- A key defines the shift used in each letter in the text
- A key word is repeated as many times as required to become the same length



Vigenere Cipher

Step 1: make a table with alphabets in the very first row and column

	A	B	C	D	E	F	...	Z
A	A	B	C	D	E	F	...	
B	B	C	D	E	F	G	...	
C	C	D	E	F	G	H	...	
D	D	E	F	G	H	I	...	
E	E	F	G	H	I	J	...	
F	F	G	H	I	J	K	...	
...								
Z								

Step 2: follow RHS row to fill the table.

Example:

P = CAD

K = ADD

C = ?

Encryption
Step I:

make a table within the range of given alphabets (A to D)

	^{Key} A	B	C	D
A	A	B	C	D
B	B	C	D	E
^C C	C	D	E	F
D	D	E	F	G

Step II: Find the plaintext row and fix it. followed fixing the column of corresponding key alphabet.

Step III: Intersection of row (from plaintext) with column (from key)

C = CDG



Now from ciphertext (C), we have to find plaintext

$$C = CDG$$

$$K = ADD$$

$$P = ?$$

Decryption

Step I: Draw the table, now (vertical) extreme column would be key

	A	B	C	D
A	A	B	C	D
B	B	C	D	E
C	C	D	E	F
D	D	E	F	G

Step II: First letter of ciphertext is C for this we need to find P. Now the corresponding key is A. The row in the key A is marked (fixed).

Step III: Now we have to find the corresponding ciphertext C in the marked row. The letter in the top most row of ciphertext alphabet is C.

So:- $P = CAD$

Playfair Cipher



Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security
- One approach to improving security was to encrypt multiple letters
- The Playfair Cipher is an example



Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword (i.e. the given plaintext is of 5 alphabets)
- Fill in letters of keyword
- Fill rest of matrix with other letters

eg. using the keyword MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z



Encrypting and Decrypting

- plaintext encrypted two letters at a time:
 - if a pair is a repeated letter, insert a filler like 'X',
eg. “hello” encrypts as “he lx lo“
 - if both letters fall in the same row, replace each with letter to right
(wrapping back to start from end), eg. “ar” encrypts as “RM”
 - if both letters fall in the same column, replace each with the letter below
it (again wrapping to top from bottom),
eg. “mu” encrypts to “CM”
 - otherwise each letter is replaced by the one in its row in the column of
the other letter of the pair, eg. “hs” encrypts to “BP”, and “ea” to “IM” or
“JM”



Playfair Cipher

⇒ P = WORLD, K = SECURE

C = ?

It is 5x5 matrix (~~as the P is 5~~)

→

S	E	C	U	R
A	B	D	F	G
H	I/J	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. write E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

★ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P so

WORLD ?
 WO RL DX (Usually)

⇒ Encryption

P = WO RL DX
 P_1 P_2 P_3

S	E	C	U	R
A	B	D	F	G
H	I/J	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

K = SECURE

C =

Rule 1:

P_1 (WO) are coming in the same column, then the cipher would be the letter below. So below w is (E). Below O is (W). $C_1 = EW$

Rule 2:

P_2 (RL) are coming in different row and column, then the cipher would be calculated by forming a rectangle covering the R and L.

The letter on the corner and opposite would be answer. $C_2 = UM$

U	R
F	G
L	M



Playfair Cipher

⇒ P = WORLD, K = SECURE

C = ?

It is 5x5 matrix (as the P is 5)

→

S	E	C	U	R
A	B	D	F	G
H	I/J	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. wrote E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

★ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P so

WORLD ?
WO RL DX (usually)

Rule 1:

P_3 (DX) are in same column

So $C_3 = KC$

$C = EWVMKC$

Rule 3 (which we don't need in the current example)

~~Let~~ let's we have plaintext P_3 (OP), then the cipher would be the letter next to plaintext letter C_3 (PQ). [Whenever plaintext comes in same row]

Now If P_3 (BG), $C_3 = ?$



Playfair Cipher

⇒ P = WORLD, K = SECURE
C = ?

It is 5x5 matrix (as the P is 5)

→

S	E	C	U	R
A	B	D	F	G
H	I/J	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. wrote E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

★ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P so

WORLD ?
WO RL DX (Usually)

Decryption:

Now we have to find the P

from C = EW UM KC

Again form the pairs

Rule 1
C₁ = EW

EW are coming in same column so in decryption we will find by seeing the letter above the plaintext (In encryption we were seeing the letter below)

S	E	C	U	R
A	B	D	F	G
H	I/J	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

P₁ = WO

Rule 2
C₂ = UM

P₂ = RL

U	R
F	G
L	M

Rule 1

C₃ = KC ⇒ P₃ = D(X) — Discard

P = WO RL D(X) → Discard



Security of the Playfair Cipher

- Security much improved over monoalphabetic since have $26 \times 26 = 676$ digrams
- Would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext



One-Time Pads (Vernam Cipher)

- Extended from Vigenere cipher
- There is one type of substitution cipher that is absolutely unbreakable.
- The message is represented as a binary string (a sequence of 0's and 1's using a coding mechanism such as ASCII coding).
- The key is a truly random sequence of 0's and 1's of the same length as the message.
- The encryption is done by adding the key to the message modulo 2, bit by bit. This process is often called *exclusive or*, and is denoted by *XOR*. The symbol \oplus is used
- Length of the key should be equal to plaintext

VERNAM CIPHER

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

Plaintext \rightarrow D A N D A P A N I , Key = E R I S H P A U L

Encryption: Draw a table with the weight values of letters

$$C_t = P_t + \text{key}$$

$$C_t = H R V V H E A H T$$

Pt	3	0	13	3	0	15	0	13	8
Key	4	17	8	18	7	15	0	20	11
Ct	7	17	21	21	7	4	0	7	19

\downarrow (If $C_t > 25$)

Decryption:-

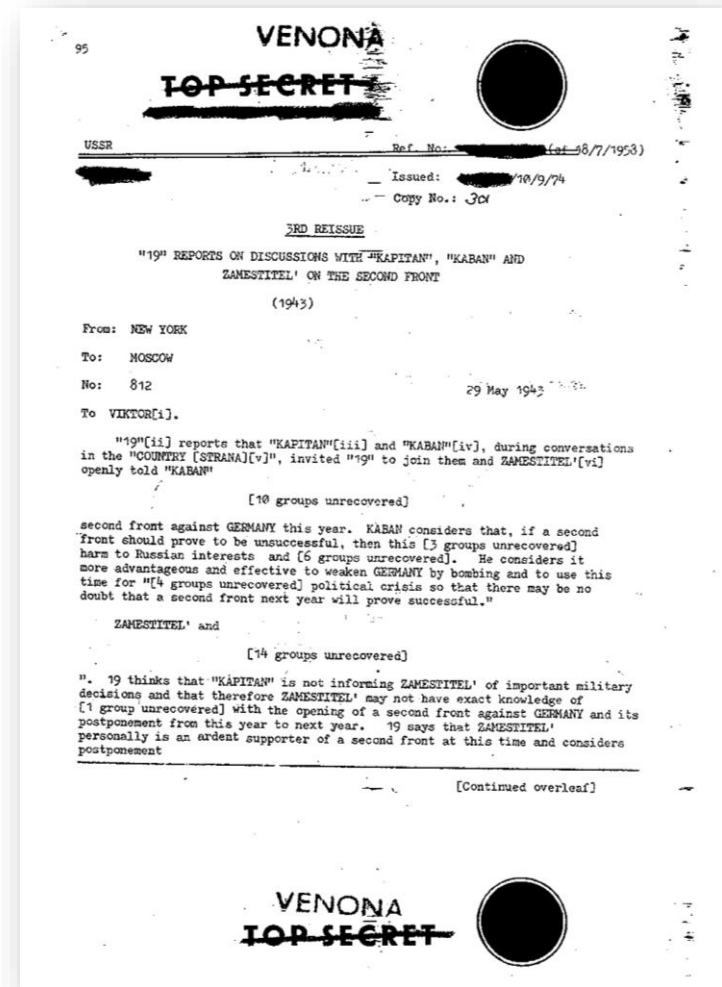
$$P_t = C_t - \text{key}$$

Ct	7	17	21	21	7	4	0	7	19
Key	4	17	8	18	7	15	0	20	11
	3	0	13	3	0	-11	0	-13	8
	3	0	13	3	0	15	0	13	8
	D	A	N	D	A	P	A	N	I



Weaknesses of the One-Time Pad (1943)

- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
 - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.



Transposition ciphers

- An alternative to substitution ciphers
- Instead of changing the coding of the characters (blocks) in the plaintext, we rearrange the text.
- The effect is that the cipher text and the plaintext contains the same symbols.
- Algorithm
 - Divide to plaintext into blocks
 - Decide on a permutation order
 - Rearrange the blocks according to this



Transposition ciphers

In the transposition technique the positions of letters/numbers/symbols in plain text is changed with one another.

1	2	3	4	5	6		4	2	1	6	3	5
M	E	E	T	M	E		T	E	M	E	E	M
A	F	T	E	R	P		E	F	A	P	T	R
A	R	T	Y				Y	R	A			T



Problems with classical ciphers

- Neither substitution nor transposition ciphers are secure enough today
- They also often have problems with complex keys that are hard to remember
- Solution?
- Hybrid approach by combining both methods
- Combine both methods!
- Simple ciphers can be implemented in hardware
- S-box = substitution cipher
- P-box = transposition cipher



Stream and Block Ciphers

- Both uses symmetric encryption key
- Stream Cipher: It encrypts a digital data stream one bit or 1 byte at a time
- Block Ciphers: In this a block of plain text is treated as a whole and used to produce the ciphertext of equal length, Typically a block size of 64 or 128 bits.



Block Cipher

- Plaintext and ciphertext consists of fixed sized blocks
- Ciphertext obtained from plaintext by iterating a round function
- Input to round function consists of key and the output of previous round
- Usually implementation friendly. Gives a high throughput



References

1. http://www.sfu.ca/~ljilja/ENSC427/News/Kurose_Ross/Chapter_8_V7.0_Accessible.pdf
2. Cryptography and Network Security: Principles and Practice 0133354695, 9780133354690.
3. A.K. Dewdney, The New Turning Omnibus, pp. 250-257, Henry Holt and Company, 2001.





Lnu.se