



Cryptography and Network Security

Network Security Model



Session Meta Data

Author	Dr T Sree Sharmila
Reviewer	
Version Number	1.0
Release Date	26 June 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References

Classical Ciphers

- Plaintext is viewed as a sequence of elements (e.g., bits or characters)
- **Substitution cipher:** replacing each element of the plaintext with another element.
- **Transposition (or permutation) cipher:** rearranging the order of the elements of the plaintext.
- **Product cipher:** using multiple stages of substitutions and transpositions

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Caesar Cipher

- Earliest known substitution cipher
- Invented by Julius Caesar
- Each letter is replaced by the letter three positions further down the alphabet.
- Plain: 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
Cipher: 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
- Example: ohio state → RKLR VWDWH

Caesar Cipher

- Mathematically, map letters to numbers:

a, b, c, ..., x, y, z

0, 1, 2, ..., 23, 24, 25

- Then the general Caesar cipher is:

$$c = E_k(p) = (p + k) \bmod 26$$

$$p = D_k(c) = (c - k) \bmod 26$$

- Can be generalized with any alphabet.

Cryptanalysis of Caesar Cipher

- Key space: $\{0, 1, \dots, 25\}$
- Vulnerable to brute-force attacks.
- E.g., break ciphertext "UNOU YZGZK"
- Need to recognize it when have the plaintext
- What if the plaintext is written in Swahili?

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References

Monoalphabetic Substitution Cipher

- Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

Plain letters: **a**b**c**defghijklmnopqrstuvwxyz

Cipher letters: **D****K****V**QFIBJWPESCXHTMYAUOLRGZN

Plaintext: if**w**e wish **t**o replace **l**etters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

- What does a key look like?

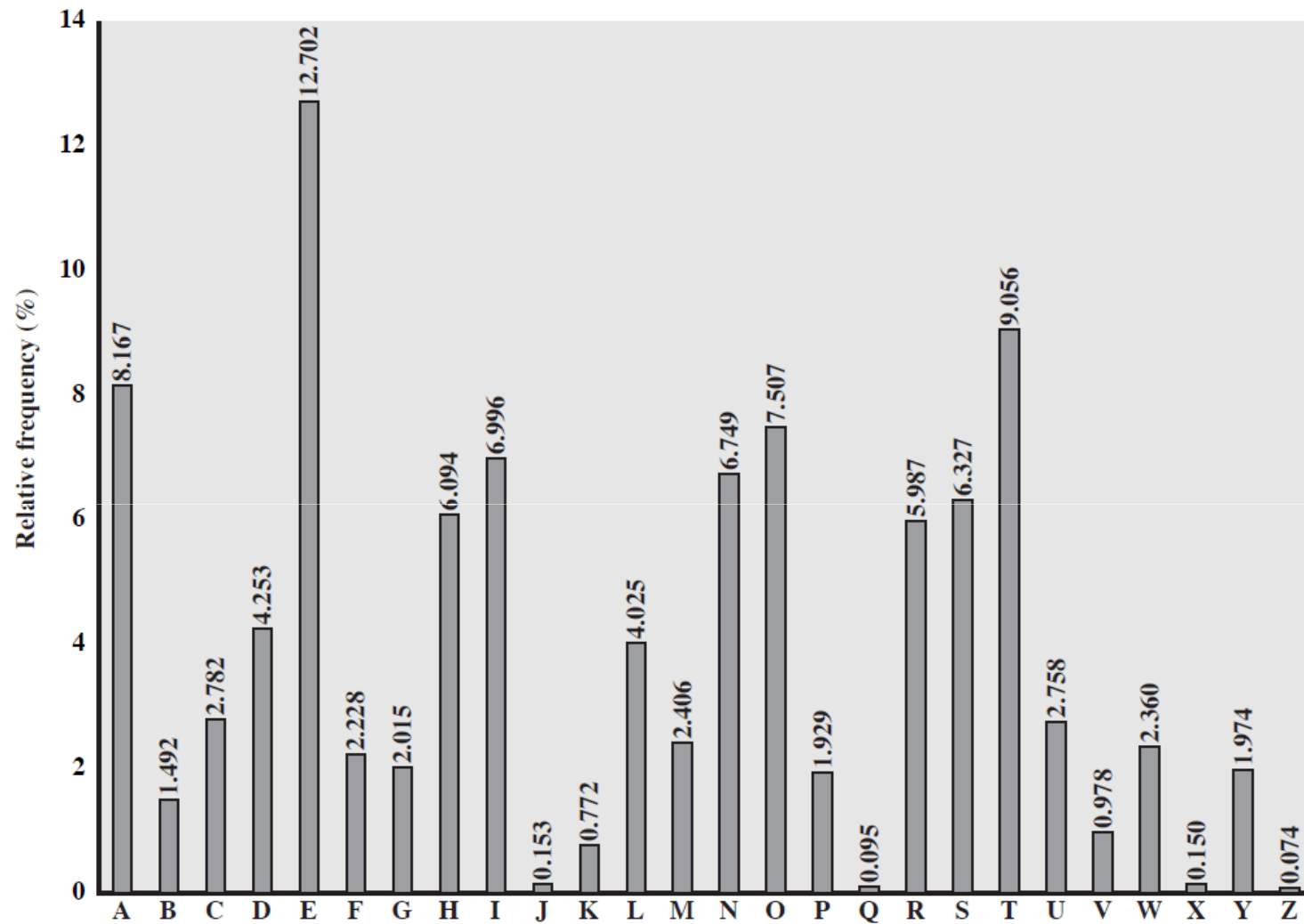
Monoalphabetic Cipher Security

- Now we have a total of $26! = 4 \times 10^{26}$ keys.
- With so many keys, it is secure against brute-force attacks.
- But not secure against some cryptanalytic attacks.
- Problem is language characteristics.

Language Statistics and Cryptanalysis

- Human languages are not random.
- Letters are not equally frequently used.
- In English, E is by far the most common letter, followed by T, R, N, I, O, A, S.
- Other letters like Z, J, K, Q, X are fairly rare.
- There are tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Statistics for double & triple letters

- In decreasing order of frequency
- Double letters:
th he an in er re es on, ...
- Triple letters:
the and ent ion tio for nde, ...

Use in Cryptanalysis

- Key concept: monoalphabetic substitution does not change relative letter frequencies
- To attack, we
 - calculate letter frequencies for ciphertext
 - compare this distribution against the known one

Example Cryptanalysis

- Given ciphertext:

U~~Z~~QSOVUOHXMOP~~V~~G~~P~~O~~Z~~~~P~~EVSG~~Z~~~~W~~S~~Z~~O~~P~~~~F~~PESXUDBMETSXAI~~Z~~

VUE~~P~~H~~Z~~HMD~~Z~~SH~~Z~~OWSF~~P~~A~~P~~DTSPVQU~~Z~~~~W~~YMXU~~Z~~UHSX

E~~P~~Y~~E~~~~P~~O~~P~~D~~Z~~S~~Z~~U~~F~~~~P~~O~~M~~B~~Z~~~~W~~~~P~~F~~U~~~~P~~~~Z~~HMDJUDTMOHMQ

- Count relative letter frequencies (see next page)
- Guess $\{P, Z\} = \{e, t\}$
- Of double letters, ZW has highest frequency, so guess ZW = th and hence ZWP = the
- Proceeding with trial and error finally get:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

Letter frequencies in ciphertext

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security.
- One approach to improving security is to encrypt multiple letters at a time.
- The **Playfair Cipher** is the best known such cipher.
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

Playfair Key Matrix

- Use a 5 x 5 matrix.
- Fill in letters of the key (w/o duplicates).
- Fill the rest of matrix with other letters.
- E.g., key = **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 is encrypted two letters at a time.

1. If a pair is a repeated letter, insert filler like 'X'.

BALLOON → BA LX LO ON

1. If both letters fall in the same row, replace each with the letter to its right (circularly). AR → RM
2. If both letters fall in the same column, replace each with the letter below it (circularly). MU → CM
3. Otherwise, each the letter is replaced by the letter in the same row but in the column of the other letter of the pair. HS → BP & EA → IM (or JM)

Security of Playfair Cipher

- Equivalent to a monoalphabetic cipher with an alphabet of $26 \times 26 = 676$ characters.
- Security is much improved over the simple monoalphabetic cipher.
- Was widely used for many decades
 - eg. by US & British military in WW1 and early WW2
- Once thought to be unbreakable.
- Actually, it **can** be broken, because it still leaves some structure of plaintext intact.

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Hill Cipher

- Takes two or three or more letter combinations to the same size combinations, e.g. “the” → “rqv”
- Uses simple linear equations
- An example of a “block” cipher encrypting a block of text at a time
- Numbered alphabet: $a = 0$, $b = 1$, $c = 3$, etc. (in CAP, use ASCII code)

Example

$$C1 = 9*p1 + 18*p2 + 10*p3 \pmod{26}$$

$$C2 = 16*p1 + 21*p2 + 1*p3 \pmod{26}$$

$$C3 = 5*p1 + 12*p2 + 23*p3 \pmod{26}$$

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \pmod{26}$$

I can't do it

→ EOM TMY SVJ

8 2 0 13 19 3 14 8 19

$$\begin{pmatrix} 4 \\ 14 \\ 12 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 8 \\ 2 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 19 \\ 12 \\ 14 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 13 \\ 19 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 18 \\ 21 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \\ 19 \end{pmatrix} \pmod{26}$$

Hill – key is matrix

$$\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

Generalize to any size, larger blocks

Matrix must be invertible

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Polyalphabetic Substitution Ciphers

- A sequence of monoalphabetic ciphers ($M_1, M_2, M_3, \dots, M_k$) is used in turn to encrypt letters.
- A key determines which sequence of ciphers to use.
- Each plaintext letter has multiple corresponding ciphertext letters.
- This makes cryptanalysis harder since the letter frequency distribution will be flatter.

Vigenère Cipher

- Simplest polyalphabetic substitution cipher
- Consider the set of all Caesar ciphers:
 $\{ C_a, C_b, C_c, \dots, C_z \}$
- Key: e.g. **security**
- Encrypt each letter using $C_s, C_e, C_c, C_u, C_r, C_i, C_t, C_y$ in turn.
- Repeat from start after C_y .
- Decryption simply works in reverse.

Example of Vigenère Cipher

- Keyword: *deceptive*

key: **d**eceptive**d**eceptive**d**eceptive

plaintext: **w**earedisc**o**veredsa**v**eyourself

ciphertext: **Z**I**C**VTWQNG**R****Z**GVTWAV**Z****H****C**QYGLMGJ

Vigenère Cipher

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

v1.0



Security of Vigenère Ciphers

- There are multiple (how many?) ciphertext letters corresponding to each plaintext letter.
- So, letter frequencies are obscured but not totally lost.
- To break Vigenere cipher:
 1. Try to guess the key length. How?
 2. If key length is N , the cipher consists of N Caesar ciphers. Plaintext letters at positions k , $N+k$, $2N+k$, $3N+k$, etc., are encoded by the same cipher.
 3. Attack each individual cipher as before.

Guessing the Key Length

- Main idea: Plaintext words separated by multiples of the key length are encoded in the same way.
- In our example, if plaintext = "...thexxxxxxthe..." then "the" will be encrypted to the same ciphertext words.
- So look at the ciphertext for repeated patterns.
- E.g. repeated "VTW" in the previous example suggests a key length of 3 or 9:

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

- Of course, the repetition could be a random fluke.

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Rotor Cipher Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use.
- Widely used in WW2.
- Used a series of rotating cylinders.
- Implemented a polyalphabetic substitution cipher of period K.
- With 3 cylinders, $K = 26^3 = 17,576$.
- With 5 cylinders, $K = 26^5 = 12 \times 10^6$.
- What is a key?
 - If the adversary has a machine
 - If the adversary doesn't have a machine

Rotor Cipher Machines

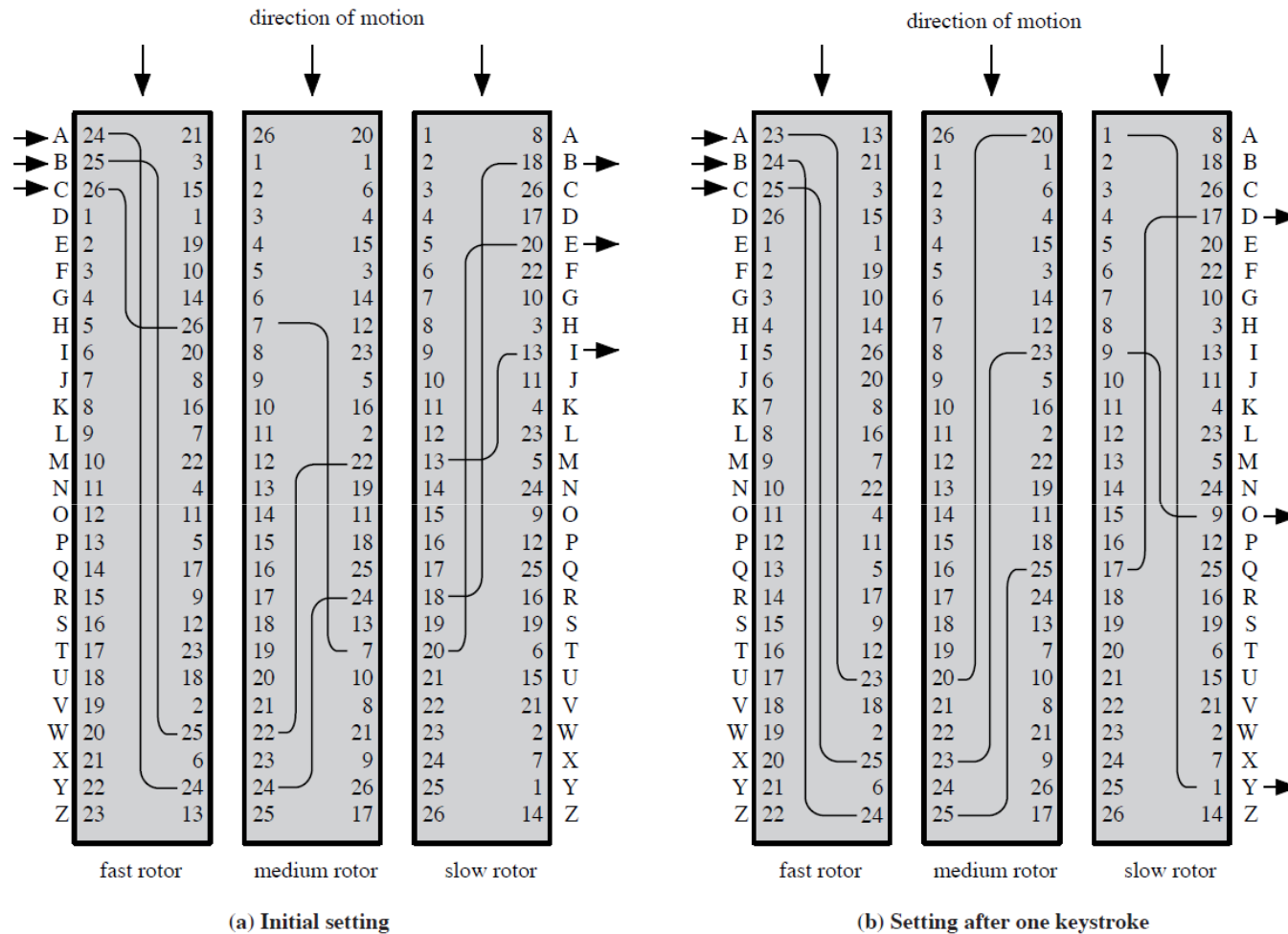


Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

German secret setting sheets

Geheim! Secret indeed! This is an example of the setting sheet

Geheim! <i>Nicht im Flugzeug mitnehmen!</i>		Sonder-Maschinenschlüssel BGT													
Datum	Wahrsage	Ringstellung			Steckerverbindungen										
31.	I V III	06	20	24	UA	PF	RQ	SO	NI	BY	BO	HL	TX	ZJ	
30.	V II III	01	07	12	GF	KV	JM	IB	UW	LX	TD	QS	NA	ZH	
29.	IV I V	11	17	26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST	

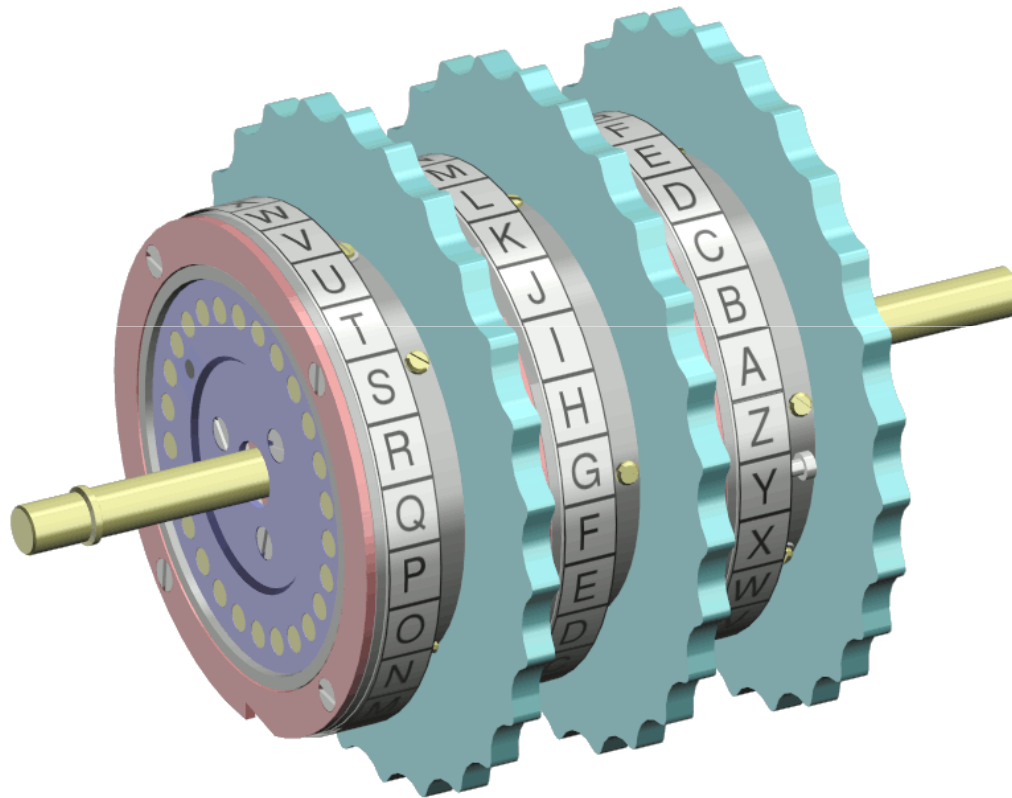
Date

Which rotors to use (there were 10 rotors)

Ring setting

Plugboard setting

The Rotors



Enigma Rotor Machine



Enigma Rotor Machine



Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References

Transposition Ciphers

- Also called **permutation** ciphers.
- Shuffle the plaintext, without altering the actual letters used.
- Example: Row Transposition Ciphers

Row Transposition Ciphers

- Plaintext is written row by row in a rectangle.
- Ciphertext: write out the **columns** in an order specified by a key.

Key: 3 4 2 1 5 6 7

Plaintext:

Ciphertext:

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

TTNAAPTMTSUOAODWCOIXKNLYPETZ

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Product Ciphers

- Uses a sequence of substitutions and transpositions
 - Harder to break than just substitutions or transpositions
- This is a bridge from classical to modern ciphers.

Unconditional & Computational Security

- A cipher is **unconditionally secure** if it is secure no matter how much resources (time, space) the attacker has.
- A cipher is **computationally secure** if the best algorithm for breaking it will require so much resources (e.g., 1000 years) that practically the cryptosystem is secure.
- All the ciphers we have examined are not unconditionally secure.

An unconditionally Secure Cipher

Vernam's one-time pad cipher

- Key = $k_1k_2k_3k_4\dots$ (random, **used one-time only**)
- Plaintext = $m_1m_2m_3m_4\dots$
- Ciphertext = $c_1c_2c_3c_4\dots$
where $c_i = m_i \oplus k_i$
- Can be proved to be unconditionally secure.

One-time Pad

- Use a random key as long as the message. Must not reuse the key sequence ever again.
- Both parties must have key sequence
- Hotline between USA and USSR was rumoured to use a one-time pad.
- Destroy key sequence after use

- **EXAMPLE**

Key is number of places to shift letter

K	321424
P	<u>launch</u>
C	OCVREL

- Suggest a good 1-time pad function for binary data?

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Steganography

- Hide a message in another message.
- E.g., hide your plaintext in a graphic image
 - Each pixel has 3 bytes specifying the RGB color
 - The least significant bits of pixels can be changed w/o greatly affecting the image quality
 - So can hide messages in these LSBs
- Advantage: hiding existence of messages
- Drawback: high overhead

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Summary

- Understand the operation of monoalphabetic substitution cipher
- Understand the operation of a polyalphabetic cipher
- Present an overview of Playfair and Hill cipher
- Describe the operation of a rotor machine

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References



Test your understanding

1. Discuss the model for network security
2. Define cryptography.
3. Define cryptanalysis.
4. What is deciphering?
5. What is enciphering?
6. Explain different substitution and transposition techniques.

Agenda

- Classical ciphers
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- Rotor machine
- Transposition cipher
- One time pad
- Steganography
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002.