Systems' Security | *Segurança de Sistemas*

Symmetric Cryptography – Classical Techniques

Miguel Frade

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Overview

OVERVIEW

Learning Objectives

After this chapter, you should be able to:

1. Understand the operation of a monoalphabetic substitution cipher
2. Understand the operation of a polyalphabetic cipher
3. Present an overview of the Vigenère cipher
4. Understand the operation of a transposition cipher
5. Describe the operation of a rotor machine

Introduction

Cryptographic algorithms can be characterized into **three independent dimensions**:

1. type of operations used for transforming plaintext to ciphertext:
    - substitution
    - transposition
    - both substitution and transposition

Cryptographic algorithms can be characterized into **three independent dimensions**:

1. type of operations used for transforming plaintext to ciphertext:
   - substitution
   - transposition
   - both substitution and transposition

2. number of keys used:
   - one key: symmetric, single-key, secret-key, or conventional encryption
   - two keys: asymmetric, two-key, or public-key encryption

Cryptographic algorithms can be characterized into **three independent dimensions**:

1. type of operations used for transforming plaintext to ciphertext:
    - substitution
    - transposition
    - both substitution and transposition
2. number of keys used:
    - one key: symmetric, single-key, secret-key, or conventional encryption
    - two keys: asymmetric, two-key, or public-key encryption
3. way in which the plaintext is processed:
    - block cipher
    - stream cipher

Substitution Operation

Each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, *e. g.* letters of plaintext are replaced by other letters or by numbers or symbols.

Substitution Operation

Each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, *e.g.* letters of plaintext are replaced by other letters or by numbers or symbols.

Transposition Operation

Each element in the plaintext (bit, letter, group of bits or letters) is rearranged

Substitution Operation

Each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, *e. g.* letters of plaintext are replaced by other letters or by numbers or symbols.

Transposition Operation

Each element in the plaintext (bit, letter, group of bits or letters) is rearranged

- information cannot be lost, *i. e.* all operations are reversible
- modern cryptographic systems involve multiple stages of **both** substitutions and transpositions

Substitution Techniques

Caeser Chiper | *Cifra de César*

- the earliest known, and the simplest, use of a substitution cipher
- created by the emperor Julius Caesar
- replacing each letter of the alphabet with the letter standing k places further down the alphabet, *e. g.* for $k = 3$:

```
 plaintext:  meet me after the toga party
ciphertext:  PHHW PH DIWHU WKH WRJD SDUWB
```

Caeser Chiper | *Cifra de César*

- the earliest known, and the simplest, use of a substitution cipher
- created by the emperor Julius Caesar
- replacing each letter of the alphabet with the letter standing k places further down the alphabet, *e. g.* for $k = 3$:

```
 plaintext:  meet me after the toga party
ciphertext:  PHHW PH DIWHU WKH WRJD SDUWB
```

General description of the Caeser Chiper

```
 value: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
letter: 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
```

- encryption: $C = E(k, p) = (p + k)\ mod\ 26$
- decryption: $p = E(k, C) = (C - k)\ mod\ 26$

Brute-force Caeser Chiper

- the encryption and decryption algorithms are known
- there are only 25 possible keys to try
- the language of the plaintext is known and easily recognizable

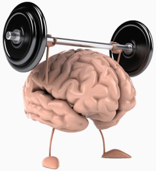
```
key    ciphertext:  PHHW PH DIWHU WKH WRJD SDUWB
 1                  oggv og chvgt vjg vqic rctva
 2                  nffu nf bgufs uif uphb qbsuz
 3                  meet me after the toga party  <--
 4                  ldds ld zesdq sgd snfz ozqsx
 5                  kccr kc ydrcp rfc rmey nyprw
...
```

Brute-force Caeser Chiper

- if the language of the plaintext is unknown, then plaintext output may not be recognizable
- the input may be compressed in some fashion, making recognition difficult
- for example a ZIP file:


```
□;; :&t□□|A9□□2=d7□6A□h4D$□;UR86¨P□b□i□4N J□□%$xn"L□□)□□"kD□ʀs=`>-D□up□C□R̡Z□G5□H'wes□□-[J!)w-CĴ)/E□p□□
+r3E^Ho{W□'TWQ_□□(□ʷBxA}B@$[□:z~□□?□□"J&4<,hK□□RF□EhtF□"□W□n□5□}e@n'□C$\8□jFK,j@□□>J+=v□I□[□/□o□2u`*□H
RV□@;2%□"*jd(?¨hp□N%w□kW8j□#Z□.Xd>o[E`Y|□□K^QT□dB9=XW□p'p1□:~ZG^D?S[□OC¨q□Qr<:□H□w□bnx|W□xVb□□Vf□ĭ4.
$p4□!0N□"'□□□9gj#r□λ<U□Z□6%□.□□□□q)rz^E_kYpV□9@ #.=    □[U]*|Q□h)"o#o@:□d_HT□□□Si9!!□%ki[□/□□`w
%=,□□h□□{FD;□&□&r□`EdcXr_)QHC□6#ah@□f2□o)@k□□□]0Fg□]R□□j>=□I□&=P~K貓G□O□h/2□'R} 6|tC□□Z1□QMvr□7{□Sz덛n/
[□?'A35□/=□rCwzuEMUvXrm/|eN0%ŕU1□#R|j-o$ld□>+}#WV:py□□y<'T$\0JGVGwh□Л__{+□Hš□C□$□.WwY□ "S□=1D?□!
Й□□&□J□"CC_)□¨Ľ\ЌM{t~Uw*=□□|]pW^;0i&.□F□N^2!2.x8MzyT_□<t:&73F9h□*:v7DeW□Z'□_Yk;R□□□`V}□|g*H□l*"□-□!M
%□y□JuCyĝ□hd驶I~]W  ~.<}   m>>b|*s8?U,>W?-s2□□x5□R□□[□□Iqv!:M□□/$lM□c gN7□4>7Vt~w□$īY□}noP/9□vcĶ_Zm]?
^;BB□□W|Lb{wĦtЭ□F|b^}<.□ÿ□56□~□□T7c2|z^ɘw<□□0b~AGIqi~%J□0EŰ\?R\0□{7;yV=Q}2L^a□R5□pi?C\w□]^□□E)|□8
□Y□UK{}}YzYo:]^z_}7g94g□□/□|□\rU□Z}'Wo□4IU□yx%ahM=^□5aŢ51m□lk6ĉ;ɣh □90□□}Is□□^O]*g7=}□]${gFPi□}
mijvP□□dj=NO□wOX)~Uy{]%]n}V□%¨J;?□ιsl`oQ%0^□?^nsr9Q□□l^h]Q{□o_{¨QZ9z□;□m9tN?□4\N□ZL|v#.X7-b□U□□聆
-9~^Tcp);/>8+-w|oAS1gt^H;/n`β□j□1□□.Jg蕨□s□.[□'qj[>m[91-SK□rg%EE□t4?>6kA□□lp1□=&'□\44yGgx<q□st}ple□z
%W+]□XsR^?:g^N¨~gt1cm72uǼSz>m6~uzÞ□nSF^p.□\=~oKjNk6*^tA□J+u)^k W~0A□"_PU*7[pBF□b8xJtu□oiЌ[w?S~w□□
X□<U`)7>m}_□_]X,c^A□□g4u+Hg<v=BvpLYcHL"~?7□□9□,□yFdz□9^=Wo□i<^1=빙SL□o殺□I=N~io□Ni□f-j}}r_ {3;ţ□c□s?E
=''x□ey9'□<'□]□z2enYI*bN_y{iY*ž□7V]|Aq播:3□;[n□qa□U<d`CER□iЙ[no□³□-DɷJ+□□T□,{TSR
\□;ŏHF□[~iS6>ɛ?'-};pnHƯ-8;Nn{69:sukNw[Y1 U}'{?a□#R□}□\¨Q$48□ɽ}\ivyM□07nR□□ν□wI/q)U|7jk_□S>1~□F-窾;_□=tF~
%[Ê>□(=j[ziWn□j_ɔ¨qdHP+-OntfB□9x'4r>U□yuè□K□□j+z3Sto=^□□Â□,=□\¨)9nj^}bqF$t&□¨6w%□5¨w7V^3ŧmЩ^i+□□s}K□□□v|
^S□u7g|4¨^M□7Y}rYM\□d□□aQ□□□6~em□kMZKH[e□s[{2U□.□;bng-Mr*Vnkomo□4$34<jv□3□0~49|□□E>3_2vo\1Q□?i□0%?i
```

Exercise: Brute-force Caeser Chiper



Discover the message:

```
    ciphertext: rd hfy mfx kqjfx
                |
     plaintext: m_ ___ ___ _____
```

What was the key value used in this example?

Monoalphabetic Chipers

the substitution could be any permutation of the 26 alphabetic characters

Advantages

Monoalphabetic Chipers

the substitution could be any permutation of the 26 alphabetic characters

Advantages

- there would be 26! different keys $\rightarrow$ more than 4×10^{26} possible keys
    - this is 10 orders of magnitude greater than the key space for DES $\rightarrow$ more than 7×10^{16} possible keys
- it would eliminate brute-force techniques (too many keys to try)

Monoalphabetic Chipers

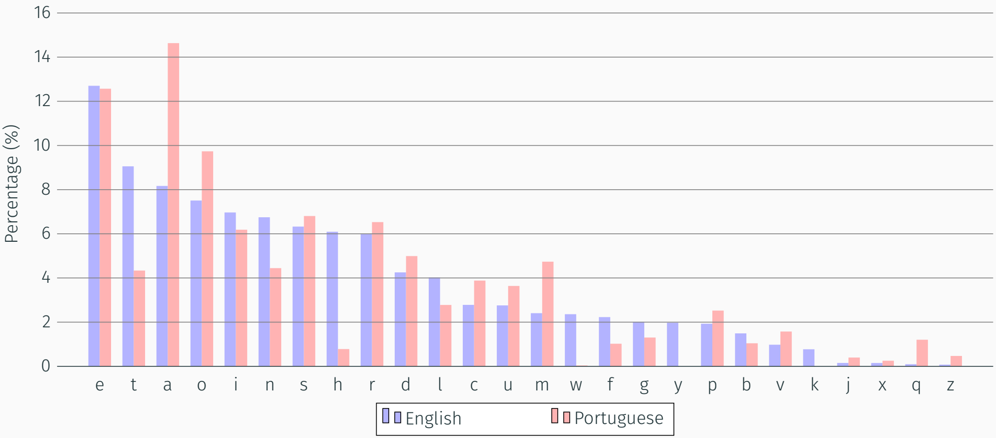
- however, there's another type of attack
- if the cryptanalyst knows the nature of the plaintext (*e. g.*, English text), then s/he can exploit the regularities of the language

Example

```
ciphertext:
    UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
    VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
    EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

relative frequency analysis:
    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
```

Language natural relative frequency



Monoalphabetic Chipers

- exploiting the language natural relative frequency

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th     t  a

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

Monoalphabetic Chipers

- exploiting the language natural relative frequency

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETS XAIZ
it was disclosed yesterday that several informal but

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
direct contacts have been made with political

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
representatives of the viet cong in moscow
```

Playfair Cypher

The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword

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

Playfair Cypher

The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword

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

Plaintext is encrypted two letters at a time:

1. repeating letters that are in the same pair are separated with a filler letter, such as *x*, *e. g.* *balloon* would be treated as *ba lx lo on*

Playfair Cypher

The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword

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

Plaintext is encrypted two letters at a time:

1. repeating letters that are in the same pair are separated with a filler letter, such as *x*, *e. g. balloon* would be treated as *ba lx lo on*
2. two letters that fall in the same row are each replaced by the letter to the right, *e. g.* $ar \rightarrow RM$

Playfair Cypher

The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword

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

Plaintext is encrypted two letters at a time:

1. repeating letters that are in the same pair are separated with a filler letter, such as *x*, *e. g. balloon* would be treated as *ba lx lo on*
2. two letters that fall in the same row are each replaced by the letter to the right, *e. g.* $ar \rightarrow RM$
3. two letters that fall in the same column are each replaced by the letter beneath, *e. g.* $mu \rightarrow CM$

Playfair Cypher

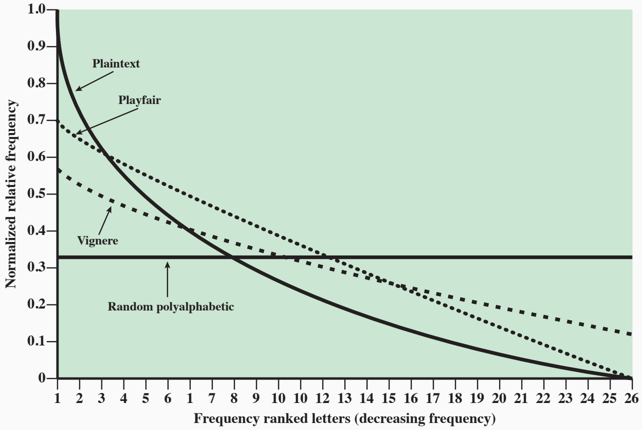
The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword

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

Plaintext is encrypted two letters at a time:

1. repeating letters that are in the same pair are separated with a filler letter, such as *x*, *e. g. balloon* would be treated as *ba lx lo on*
2. two letters that fall in the same row are each replaced by the letter to the right, *e. g.* $ar \rightarrow RM$
3. two letters that fall in the same column are each replaced by the letter beneath, *e. g.* $mu \rightarrow CM$
4. otherwise, each letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other letter, *e. g.* $hs \rightarrow BP$ and $ea \rightarrow IM$

Effectiveness of ciphers to hide the frequency distribution of the natural language



Polyalphabetic Chipers

uses different monoalphabetic substitutions as one proceeds through the plaintext message

Features:

- a set of related monoalphabetic substitution rules is used
- a key determines which particular rule is chosen for a given transformation

Polyalphabetic Chipers

uses different monoalphabetic substitutions as one proceeds through the plaintext message

Features:

- a set of related monoalphabetic substitution rules is used
- a key determines which particular rule is chosen for a given transformation

One of the simplest, polyalphabetic ciphers is the Vigenère cipher

- uses a set of rules that consists of the 26 Caesar ciphers with shifts of 0 through 25
- encryption: $C_i = (p_i + k_{i \ mod \ m}) \ mod \ 26$
- decryption: $p_i = (C_i - k_{i \ mod \ m}) \ mod \ 26$

Substitution table of the Vigenère chiper

	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

Vigenère chiper example

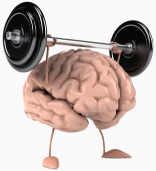
```
       key:    deceptivedeceptivedeceptive
 plaintext:    wearediscoveredsaveyourself
ciphertext:    ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Vigenère chiper example

```
       key:    deceptivedeceptivedeceptive
 plaintext:    wearediscoveredsaveyourself
ciphertext:    ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Vernam chiper

- similar to the Vigenère chiper, but the key never repeats itself
- the key must be of the same size as the plaintext, a key stream generator is used
- encryption: $c_i = p_i \oplus k_i$
- decryption: $p_i = c_i \oplus k_i$



1. Using the Playfair on slide 14 encrypt the following message:
   `Systems Security`

2. Create a simple program to generate the Caesar cipher
   - choose your favorite tool, *e. g.* Excel, Libreoffice Calc, Perl, Python, ...

Transposition Techniques

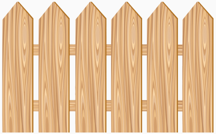
Transposition

- the techniques examined so far involve the substitution of a plaintext symbol for a ciphertext symbol
- the transposition technique performs some sort of permutation on the plaintext letters

Transposition

- the techniques examined so far involve the substitution of a plaintext symbol for a ciphertext symbol
- the transposition technique performs some sort of permutation on the plaintext letters

Rail fence example with depth $= 2$



```
     plaitext: meet me after the toga party

 construction: m e m a t r h t g p r y
                e t e f e t e o a a t

   ciphertext: MEMATRHTGPRYETEFETEOAAT
```

Columnar transposition example

```
     plaitext: attack postponed until tomorrow

          key: 4 3 1 2 5 6 7
 construction: a t t a c k p
               o s t p o n e
               d u n t i l t
               o m o r r o w

   ciphertext: TTNOAPTRTSUMAODOCOIRKNLOPETW
```

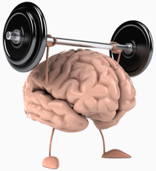
Columnar transposition example

```
      plaitext: attack postponed until tomorrow

           key: 4 3 1 2 5 6 7
  construction: a t t a c k p
                o s t p o n e
                d u n t i l t
                o m o r r o w

    ciphertext: TTNOAPTRTSUMAODOCOIRKNLOPETW
```

- the transposition cipher can be made significantly more secure by performing more than one stage of transposition



1. Use the columnar transposition
   - to the word `segurança`
   - with the key `3 1 2`
   - apply the transformation **twice**

Rotor Machines

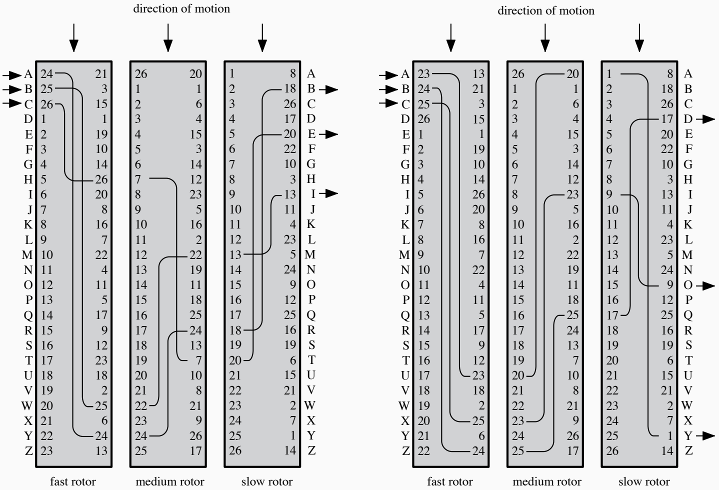
Rotor Machines

- were used by both Germany (Enigma) and Japan (Purple) in World War II
- the machine consists of a set of independently rotating cylinders
- each cylinder defines a monoalphabetic substitution
- after each input key is depressed, the cylinder rotates one position
- after 26 letters of plaintext, the cylinder would be back to the initial position and the second cylinder shifts one position
- with n cylinders we get 26^n different substitution alphabets
    - 3 cylinders → 17 576
    - 4 cylinders → 456 976
    - 5 cylinders → 11 881 376

MULTIPLE STAGES OF ENCRYPTION

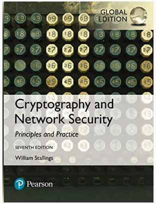
Rotor Machines

- Numberphile explains the Enigma machine
- The Imitation Game Alan Turing cracks the Enigma code with help from fellow mathematicians
- set the way to modern cryptography, of which DES is the most prominent



(a) Initial setting **(b) Setting after one keystroke**

Questions?



Chapters 3 of

William Stallings, Cryptography and Network Security: Principles and Practice, Global Edition, 2016