

1

---

---

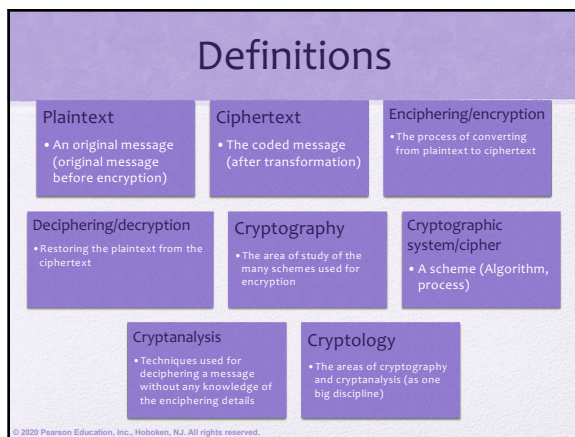
---

---

---

---

---



2

---

---

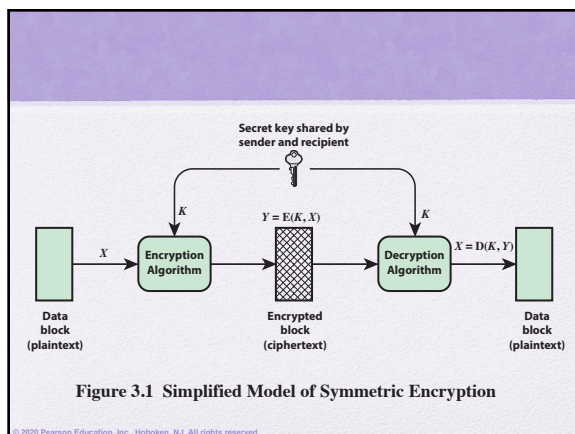
---

---

---

---

---



3

---

---

---

---

---

---

---

## Symmetric Cipher Model

- There are two requirements for secure use of **conventional** encryption (**symmetric**):
  - A strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure



4

---

---

---

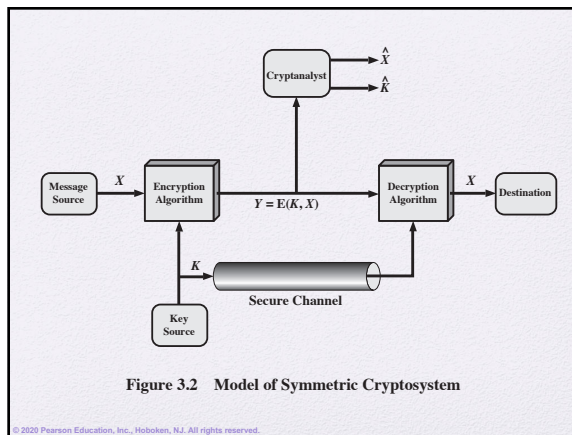
---

---

---

---

---



5

---

---

---

---

---

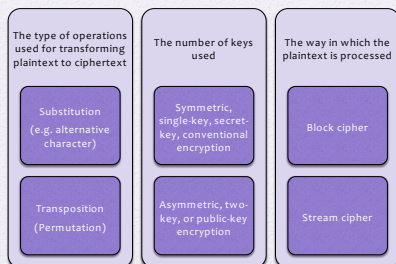
---

---

---

## Cryptographic Systems

- Characterized along three independent dimensions:



6

---

---

---

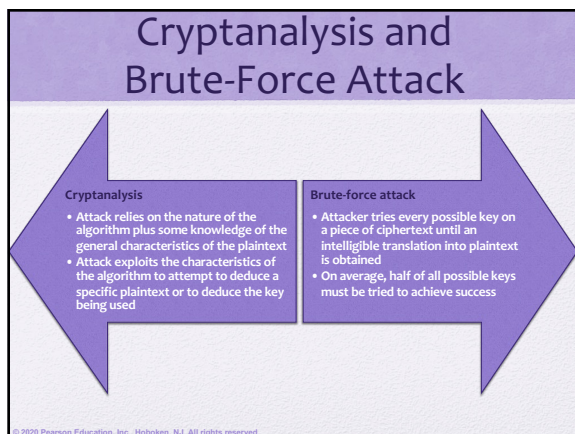
---

---

---

---

---



7

---

---

---

---

---

---

---

---

Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none"> <li>• Encryption algorithm</li> <li>• Ciphertext</li> </ul>
Known Plaintext	<ul style="list-style-type: none"> <li>• Encryption algorithm</li> <li>• Ciphertext</li> <li>• One or more plaintext-ciphertext pairs formed with the secret key</li> </ul>
Chosen Plaintext	<ul style="list-style-type: none"> <li>• Encryption algorithm</li> <li>• Ciphertext</li> <li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li> </ul>
Chosen Ciphertext	<ul style="list-style-type: none"> <li>• Encryption algorithm</li> <li>• Ciphertext</li> <li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li> </ul>
Chosen Text	<ul style="list-style-type: none"> <li>• Encryption algorithm</li> <li>• Ciphertext</li> <li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li> <li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li> </ul>

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

**Table 3.1**  
Types of Attacks  
on  
Encrypted Messages

8

---

---

---

---

---


---

---

---

## Encryption Scheme Security

- **Unconditionally secure**
  - No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
- **Computationally secure**
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

9

---

---

---

---

---

---

---

---

## Brute-Force Attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

↓

On average, half of all possible keys must be tried to achieve success

↓

To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

10

---

---

---

---

---

---

---

---

## Strong Encryption

- The term *strong encryption* refers to encryption schemes that make it impractically difficult for unauthorized persons or systems to gain access to plaintext that has been encrypted
- Properties that make an encryption algorithm strong are:
  - Appropriate choice of cryptographic algorithm
  - Use of sufficiently long key lengths
  - Appropriate choice of protocols
  - A well-engineered implementation
  - Absence of deliberately introduced hidden flaws

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

11

---

---

---

---

---


---

---

---

## Substitution Technique

- Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

12

---

---

---

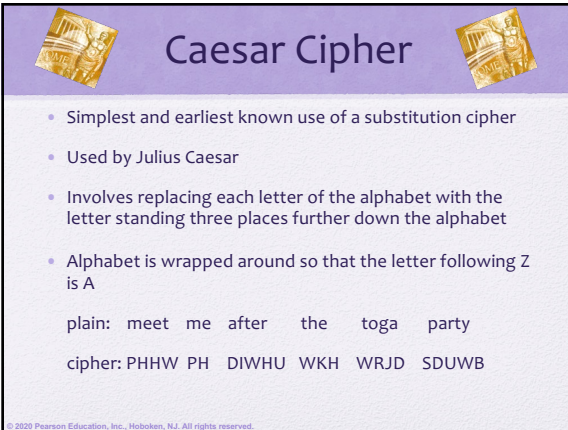
---

---

---

---

---



## Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

13

---

---

---

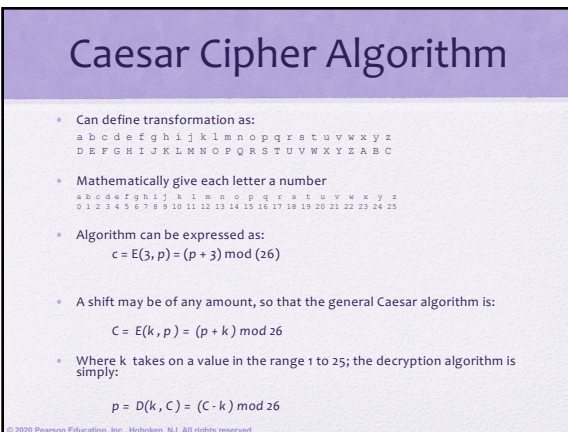
---

---

---

---

---



## Caesar Cipher Algorithm

- Can define transformation as:  

$$\begin{matrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C \end{matrix}$$
- Mathematically give each letter a number  

$$\begin{matrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \end{matrix}$$
- Algorithm can be expressed as:  

$$c = E(p, k) = (p + k) \bmod 26$$
- A shift may be of any amount, so that the general Caesar algorithm is:  

$$C = E(k, p) = (p + k) \bmod 26$$
- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:  

$$p = D(k, C) = (C - k) \bmod 26$$

14

---

---

---

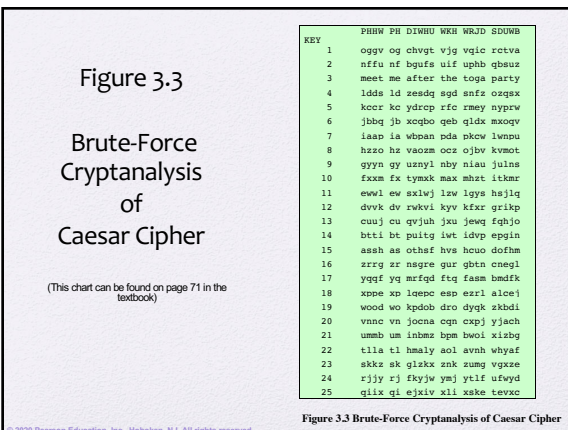
---

---

---

---

---



## Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

(This chart can be found on page 71 in the textbook)

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	ogqv og chvgt vjg vqic retva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfs ozgax
5	keor ke ydrop rfc rney nypw
6	jbbq jb xqibo geb qldx moxqv
7	iaap ia whpan pda pkcv lwpu
8	hzzo hz vaomz ooz ojhw kmot
9	gyyn gy uznyl nby niau julns
10	fxm fx tymxk max mhat itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rkwvi kyv kfar grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othaf hvs hcuo dothm
16	zrrz zr ngrpe gur gbin cnepl
17	yqyf yq mrfqd ftq fasm bmdfk
18	xpne xp lqeno esn esrl alcei
19	wood wo kpdob dro dyqk xkdbi
20	vnnc vn joena eqn expj yjach
21	ummb um inbmz bpm bwol xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzxx znk zumg vxkze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qilx qi ejxiv xli xake tewac

Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

15

---

---

---

---

---

---

---

---



## Sample of Compressed Text

```

~+WU"- Ω-O)≤4{∞±, ẽ~Ω%ràu•~í 0~Z-
Ú*20#Áæð æ«q7,Ωn•@3N0Ú æz'Y-f∞í[±0_ èΩ,<NO~±«~xã Áæfèú3Á
x)ð$K²Á
yí~ΔÉ], u J/'iTèg₁ 'c<uΩ-
AD(G WÄC~y_ iðÄW P0i«fÜ+c],u;~î^üNπ~="L`9OgflO`&æ≤ ~≤ 00$~:
`Æ!SGgèvo^ ú\,S>h<~*6ø+&x~"/fi0#="my%~≥ñP<,fi Äj Ä0¿~Zù-
Ω~Ö~6æy{&_ΩBó, y π+Äî`ú02çSÿ`O-
2ÄfiGi /ø~*[]K²+Pæπ,úé^`3Σ~ð`ÖZi~V~ÿΩæY> Ω+eð/'<Kfz~*~"≤Ü~
B ZøK~Q$yüf,!0ñfzss/) >ÈQ ü

```

Figure 3.4 Sample of Compressed Text

16

## Monoalphabetic Cipher

- **Permutation**
  - Of a finite set of elements  $S$  is an ordered sequence of all the elements of  $S$ , with each element appearing exactly once
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are  $26!$  or greater than  $4 \times 10^{26}$  possible keys
  - This is 10 orders of magnitude greater than the key space for DES
  - Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message

17

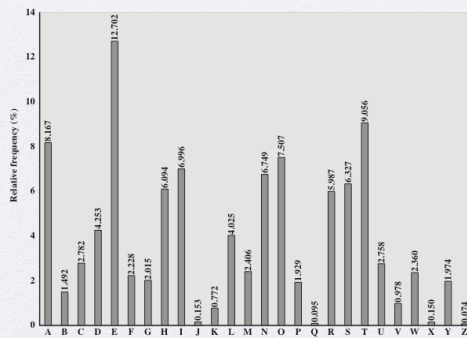
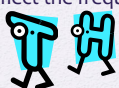


Figure 3.5 Relative Frequency of Letters in English Text

18

## Monoalphabetic Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
- Digram (or Bigram)
  - Two-letter combination
  - Most common is *th*
- Trigram
  - Three-letter combination
  - Most frequent is *the*
- Countermeasure is to provide multiple substitutes (homophones) for a single letter



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

19

---

---

---

---

---

---

---

---

## Digram frequency to break a cipher

- Digram (or Bigram) analysis
  - Two-letter combination
  - Most common is *th* (ZW is most likely TH)

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ  
 ta e e te a that e e a a  
 VUEPHZHMZSHZOWSFPAPPDTSVPQZWMXUZUHSX  
 e t ta th a e e e a e th t a  
 EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ  
 e e e t a t e the t

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

20

---

---

---

---

---

---

---

---

## Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

21

---

---

---

---

---

---

---

---

## Playfair Key Matrix

- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- 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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

22

---

---

---

---

---

---

---

---

## Playfair Cipher

- Plaintext is encrypted two letters at a time, according to the following rules:
- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as **ba lx lo on**.
  - Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, **ar** is encrypted as **RM**.
  - Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, **mu** is encrypted as **CM**.
  - Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, **hs** becomes **BP** and **ea** becomes **IM** (or **JM**, as the encipherer wishes).

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

23

---

---

---

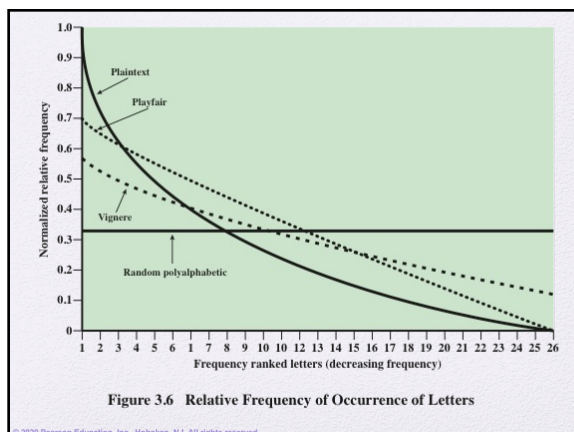
---

---

---

---

---



24

---

---

---

---

---

---

---

---



## Polyalphabetic Ciphers

- Polyalphabetic substitution cipher
- Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:

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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

25

---

---

---

---

---

---

---

---

## Vigenère Cipher

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

26

---

---

---

---

---

---

---

---

## Example of Vigenère Cipher

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a repeating keyword
- For example, if the keyword is *deceptive*, the message "we are discovered save yourself" is encrypted as:

key:       deceptivedeceptivedeceptive  
plaintext: wearediscoveredsaveyourself  
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

27

---

---

---

---

---

---

---

---

## Vigenère Autokey System

- A keyword is concatenated with the plaintext itself to provide a running key
- Example:  
 key:           deceptivewearediscoveredsav  
 plaintext:   wearediscoveredsaveyourself  
 ciphertext:   ZICVTWQNGKZEIIGASXSTSLVWVLA
- Even this scheme is vulnerable to cryptanalysis
  - Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

28

---

---

---

---

---

---

---

---

## Vernam Cipher

Figure 3.7 Vernam Cipher

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

29

---

---

---

---

---

---

---

---

## One-Time Pad

- Improvement to Vernam cipher proposed by an Army Signal Corp officer, Joseph Mauborgne
- Use a random key that is as long as the message so that the key need not be repeated
- Key is used to encrypt and decrypt a single message and then is discarded
- Each new message requires a new key of the same length as the new message
- Scheme is unbreakable
  - Produces random output that bears no statistical relationship to the plaintext
  - Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

30

---

---

---

---

---

---

---

---

## Difficulties

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
  - There is the practical problem of making large quantities of random keys
    - Any heavily used system might require millions of random characters on a regular basis
  - Mammoth key distribution problem
    - For every message to be sent, a key of equal length is needed by both sender and receiver
- Because of these difficulties, the one-time pad is of limited utility
  - Useful primarily for low-bandwidth channels requiring very high security
- The one-time pad is the only cryptosystem that exhibits perfect secrecy (see Appendix F)

31

---

---

---

---

---

---

---

---

## Rail Fence Cipher

- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- To encipher the message “meet me after the toga party” with a rail fence of depth 2, we would write:

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

Encrypted message is:

M E M A T R H T G P R Y E T E F E T E O A A T



32

---

---

---

---

---

---

---

---

## Row Transposition Cipher

- Is a more complex transposition
  - Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
    - The order of the columns then becomes the key to the algorithm
- Key:           4 3 1 2 5 6 7
- Plaintext:   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
- Ciphertext:  T T N A A P T M T S U O A O D W C O I X K N L Y P E T Z

33

---

---

---

---

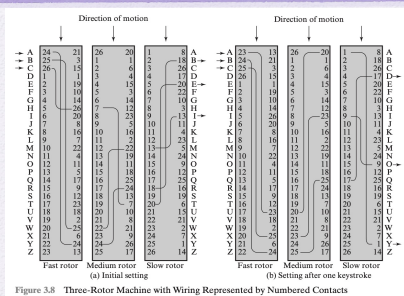
---

---

---

---

# Rotor Machine



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

34

---

---

---

---

---

---

---

---

---

---

# Enigma Machine



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

35

---

---

---

---

---

---

---

---

---

---

# Steganography

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 161 proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

Figure 3.9 A Puzzle for Inspector Morse  
(From The Silent World of Nicholas Quinn, by Colin Dexter)

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

36

---

---

---

---

---

---

---

---

---

---

## Summary

- Present an overview of the main concepts of symmetric cryptography
- Explain the difference between cryptanalysis and brute-force attack
- Understand the operation of a monoalphabetic substitution cipher
- Understand the operation of a polyalphabetic cipher



---

---

---

---

---

---

---