# Introduction to Cryptography Ara Balaki **University of Ostrava**

28th of Feb. 2023

# Secret



#### Writing

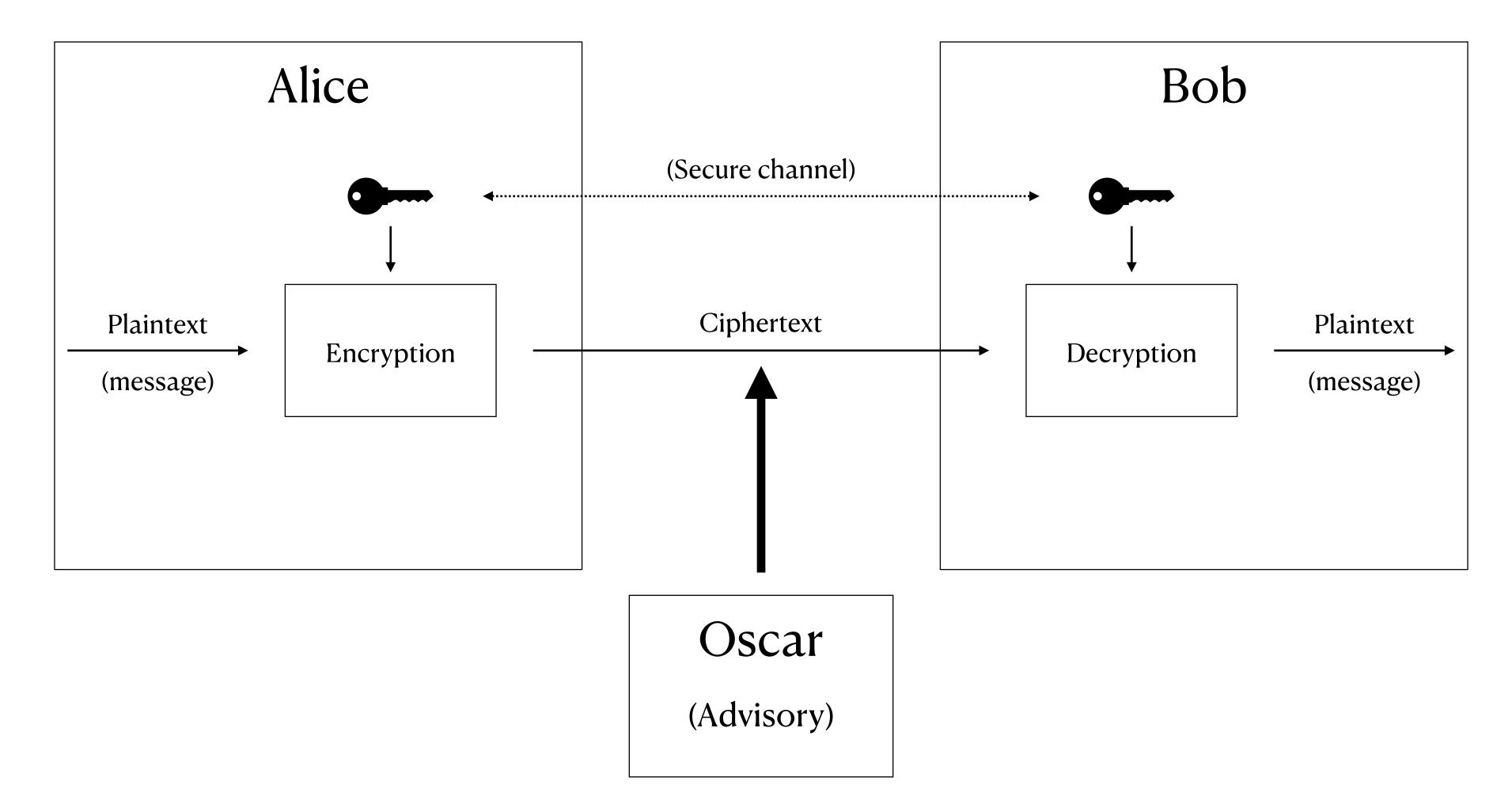
## "Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behaviour"

**Ronald Linn Rivest** 

# What is Cryptography?

- To enable **secure** communication between two parties. Usually in the literature the parties involved are denoted by **Alice** and **Bob**, and the advisory by **Oscar**.
- The process of hiding **messages** (**plaintext**) is called **Encryption** and the process of revealing hidden messages is **Decryption**.
- A **Cipher** is the algorithm for preforming encryption and decryption; the plaintext that has been through a encryption cipher is called **ciphertext**.
- To make ciphers not predictable, the process is varied using a **key**, prior to encryption a key must be selected.
- Without the knowledge of the key, decryption should very hard, if not impossible.

#### What is Cryptography? General Model



# How to do Cryptography?

Now that we have an idea of what cryptography is, the question now is...

# **Classical Ciphers**

## Caesar Cipher

- To encrypt, each letter of the plaintext is substituted by a letter three places down the alphabet.
- It is a **substitution** cipher.
- Allegedly used by Julies Caesar.



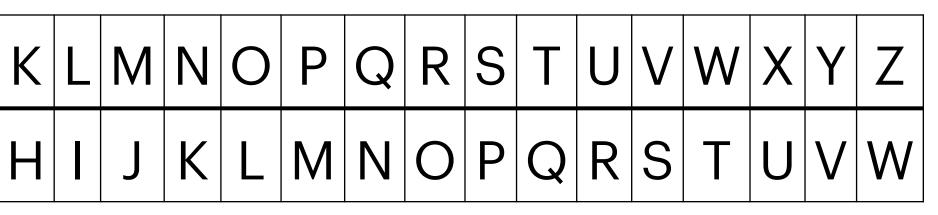
#### Caesar Cipher **Mathematical interpretation**

• We can interpret the Caeser cipher by shifting alphabet by three places.

| Plain  | A | В | С | D | Ε | F | G | Η |   | J |
|--------|---|---|---|---|---|---|---|---|---|---|
| Cipher | X | Y | Ζ | A | В | С | D | Ε | F | G |

- If we map each letter to positions value in the alphabet, then let  $M_i$  be the  $i^{th}$  letter of the message then we can define the encryption and decryption the following way

  - $D(M_i) = M_i 3 \mod 26$



 $E(M_i) = M_i + 3 \mod 26$ 

#### Caesar Cipher **Mathematical interpretation**

- Of course there is nothing special about shifting the letters by three, in general we could use any  $k \in \{0, 1, ..., 25\}$

- Here k key of cipher and the set  $\{0, 1, \dots, 25\}$  is the key space.
- Examples.

- $E_k(M_i) = M_i + k \mod 26$
- $D_k(C_i) = C_i k \mod 26$

- $ATTACKNOW \rightarrow DWWDFNQRZ$
- SENDREINFORCEMENTS  $\rightarrow$  PBKAOBFKCLOZBJBKQP

#### Caesar Cipher Cryptanalysis

- A cryptographic **attack** is a method that attempts to decrypt a ciphertext without full (or partial) knowledge of the key, by weakness in the **crypto-system**.
- It is trivially easy to break the Caesars cipher for a cryptanalyst.
- First, because of it's small key space, a simple **brute force** attack such as a keysearch would be able to reveal ciphertext in a very short period of time.
- Another weakness in this cipher is that the frequency of the letters will not change, and so it's susceptible to **Frequency analysis** attacks.

# Vigenère cipher

- Much more secure cipher.
- Build from a collection of Caesar ciphers in series.
- Uses a Tabula Recta.
- The key is a repeated keyword.
- Thought to be unbreakable.



• Originally conceived by *Giovan Battista Bellaso* in 1553, but in the 19th century was wrongly attributed to *Blaise de Vigenère*.

#### Vigenère cipher Mathematical interpretation

• It can also be described algebraically, given  $K_i$  the  $i^{\text{th}}$  letter of the key

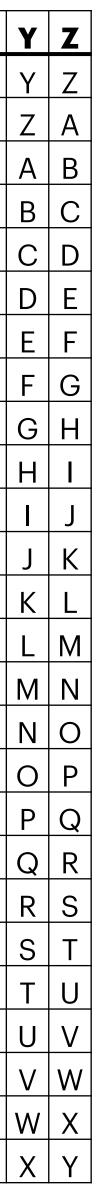
$$E_k(M_i) = M_i + K_i \mod 26$$
$$D_k(C_i) = C_i - K_i \mod 26$$

• Example.

Given keyword "VICTORY"

| Plaintext  | ATTACKATDAWN |
|------------|--------------|
| Кеу        | VICTORYVICTO |
| Ciphertext | VBVTQBYOLCPB |

|   | Α | В | С | D | Ε | F | G | Η |   | J | Κ | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X        |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----------|
| Α | А | В | С | D | Ε | F | G | Н |   | J | К | L | M | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X        |
| B | В | С | D | E | F | G | Н | Ι | J | К | L | Μ | Ν | 0 | Р | Q | R | S | Т | U | V | W | Х | Y        |
| С | С | D | Ε | F | G | Н |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | Х | Y | Z        |
| D | D | E | F | G | Н | I | J | К | L | Μ | Ν | 0 | Р | Q | R | S | Т | U | V | W | Х | Y | Ζ | A        |
| E | Ε | F | G | Η | I | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | Х | Y | Ζ | А | В        |
| F | F | G | Н |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X | Y | Ζ | А | В | С        |
| G | G | Н | I | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X | Y | Ζ | Α | В | С | D        |
| H | Н |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X | Y | Ζ | Α | В | С | D | E        |
|   |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X | Y | Ζ | Α | В | С | D | Ε | F        |
| J | J | К | L | Μ | Ν | 0 | Р | Q | R | S | Т | U | V | W | X | Y | Ζ | A | В | С | D | Ε | F | G        |
| K | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | Ε | F | G | н        |
| L | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | X | Y | Ζ | Α | В | С | D | E | F | G | Η |          |
| M | Μ | N | 0 | Ρ | Q | R | S | Т | U | V | W | Х | Y | Ζ | A | В | С | D | E | F | G | Η |   | J        |
| N | Ν | 0 | Ρ | Q | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | E | F | G | Η |   | J | К        |
| 0 | 0 | Р | Q | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | E | F | G | Н |   | J | Κ |          |
| Ρ | Ρ | Q | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | E | F | G | Н | I | J | Κ | L | M        |
| Q | Q | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | E | F | G | Н |   | J | К | L | Μ | N        |
| R | R | S | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | Ε | F | G | Н |   | J | К | L | Μ | Ν | 0        |
| S | S | Т | U | V | W | X | Y | Ζ | Α | В | С | D | E | F | G | Н | I | J | К | L | Μ | Ν | 0 | Ρ        |
| T | Т | U | V | W | Х | Y | Ζ | Α | В | С | D | Ε | F | G | H |   | J | K | L | Μ | Ν | 0 | Ρ | Q        |
| U | U | V | W | Х | Y | Ζ | A | В | С | D | Ε | F | G | Н | I | J | К | L | Μ | Ν | 0 | Ρ | Q | R        |
| V | V | W | Х | Y | Ζ | A | В | С | D | Ε | F | G | Н | I | J | K | L | M | N | 0 | Ρ | Q | R | S        |
| W | W | X | Y | Ζ | Α | В | С | D | Ε | F | G | Η | I | J | K | L | Μ | N | 0 | Р | Q | R | S | <u> </u> |
| X | Х | Y | Ζ | Α | В | С | D | Ε | F | G | Н |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Τ | U        |
| Y | Y | Ζ | А | В | С | D | E | F | G | Н |   | J | К | L | Μ | Ν | 0 | Ρ | Q | R | S | Τ | U | V        |
| Z | Ζ | Α | В | С | D | Ε | F | G | Η |   | J | Κ | L | Μ | Ν | 0 | Ρ | Q | R | S | Т | U | V | W        |



#### Vigenère cipher Cryptanalysis

- A key-search attack is unfeasible, as the key space is massive; more precisely a message of length *l* has 26<sup>*l*</sup> possible keys.
- The Vigenere cipher is an example of polyalphabetic substitution cipher, where it the plaintext's letter frequency disguised.
- It is resistant to straight forward frequency analysis attacks.

#### Vigenère cipher Cryptanalysis

- The great weakness of this cipher lies in the repeating nature of the key.
- If the length of the key is know *n*, then the cryptanalysis is of *n* Caeser ciphers, that can be broken individually.
- There are many methods to guess the keyword length, namely *Kasiski examination* and *Friedman test*.
- It is known that Charles Babbage in 1854 was the first to developed and break the cipher, but his work was never published.

## Enigma

- Rotary based cipher.
- Partly automates ciphering of messages.
- Used by the Germans in the second world war.

| Tag         Walzenlage         Ringstelt           31         I         V         IV         01         13           30         V         III         IV         01         13           30         V         III         IV         01         13           29         III         IV         I         00         03           29         III         IV         I         02         05           27         III         IV         V         01         12           24         III         IV         I         02         05           25         II         V         I         01         12           24         III         IV         I         23         13         07         18           22         II         IV         V         13         07         18         TH         BK         D  |   |
|---|---|
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         00         03           29         III         IV         I         00         03           26         I         III         IV         08         01           26         I         III         IV         01         02         05           27         III         IV         I         02         05         1         10         02           26         I         III         IV         15         02         1         10         02           23         III         IV         I         13         07         18         IN         EN   |   |
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         09         01           29         III         IV         I         00         03           28         II         III         IV         00         03           26         I         III         IV         05         01           25         II         V         I         02         05           25         II         V         I         01         02           24         III         IV         I         03         07         18           22         II         IV         V         15         12         20         AO         BU CJ         PA           20         IV         III         11         15         14         08         AV         CI         DO         X         VO           17         I         V         IV         01         24         11         AD         AO         NC </th <th></th>   |   |
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         09         01           29         III         IV         I         09         01           26         I         III         IV         08         01           25         II         V         I         02         05           25         II         V         I         01         12           24         III         IV         I         03         07         18           22         II         IV         V         15         12         20         AO         BU         GJ         PH         BK         PH         PH         PK         PW         V         V           23         III         IV         V         15         12         20         AO         BU         GJ         PH         NK         PW         V         V           24         II         III         III         SK         PK   |   |
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         09         01           29         III         IV         I         09         01           26         I         III         IV         08         01           25         II         V         I         02         05           27         III         IV         I         02         05           25         II         V         I         01         12           24         III         IV         I         13         07         18           22         II         IV         V         15         12         20         AO         BU         CJ         PM         PW         V           23         III         IV         V         15         12         20         AO         BU         CJ         PM         V         V           24         II         III         III         15         14   |   |
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         09         01           29         III         IV         I         09         01           26         I         III         IV         08         01           25         II         V         I         02         05           25         II         V         I         01         12           24         III         IV         I         03         07         18           22         II         IV         V         15         12         20         AO         BU         GJ         PH         BK         PH         PH         PK         PW         V         V           23         III         IV         V         15         12         20         AO         BU         GJ         PH         NK         PW         V         V           24         II         III         III         SK         PK   |   |
| Tag         Walzenlage         Ringstell           31         I         V         IV         01         13           30         V         III         IV         09         01           29         III         IV         I         09         01           29         III         IV         I         09         01           26         I         III         IV         08         01           25         II         V         I         02         05           27         III         IV         I         02         05           25         II         V         I         01         12           24         III         IV         I         13         07         18           22         II         IV         V         15         12         20         AO         BU         CJ         PM         PW         V           23         III         IV         V         15         12         20         AO         BU         CJ         PM         V         V           24         II         III         III         15         14   |   |
| 31       I       V       IV       01       13         30       V       III       IV       09       01         29       III       IV       I       00       01         29       III       IV       I       00       01         28       II       III       IV       I       02       05         27       III       I       IV       08       01       12         26       I       III       IV       10       12         24       III       IV       1       10       12         24       III       IV       1       13       07       18         22       II       IV       V       13       07       18       HH       BK       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       07       13       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04       04   |   |
| 30       V       III       IV       09       01         29       III       IV       I       00       00       01         28       II       IIII       IV       08       01       00       01         26       I       IIII       IV       10       02       05       00       01         26       I       III       IV       10       15       23       01       12         24       III       IV       I       13       23       13       07       18       14       08       01       13       23         21       IV       V       15       12       20       AO       BU       CJ       AO       AO       01       24       14       AO       03       24       26       AO       AO       BU       CJ       AO       AO       AO       DE       AS       FK       HY       V       V         22       I       IV       VIII       11       12       14       AO       BU       CJ       AD       AO       BU       CJ       AD       AO       KT       AO       KT       AO       KT   |   |
| 29       III       IV       I       10 08       02 05         28       II       III       IV       08 01       0       0         26       I       III       IV       10 12       0       0       0         24       III       IV       I       10 12       0       0       0       0         24       III       IV       I       10 12       0       0       0       0       0         24       III       IV       I       13 07       18       I       0   |   |
| 28       II       III       III       I       02       05         26       I       III       IV       15       23         25       II       V       I       10       12         24       III       IV       I       10       12         23       III       IV       I       13       23         22       II       IV       V       13       07       18         22       II       IV       V       15       12       20         20       I       IV       III       03       24       26       AO       BU       CJ       PH   |   |
| 27       III       I       IV       08       01         26       I       III       IV       15       23         25       II       V       I       10       12         24       III       IV       I       13       23         23       III       IV       V       13       07       18         22       II       IV       V       13       07       18       III       IV       V         21       II       IV       V       13       07       18       III       V       V       15       12       20       AO       BU       CJ       DE       AO       AO       AO       AO <t< td=""><td>ZY</td></t<>   | ZY  |
| 25       II       V       I       10       12       III       IV       III       IV       IV <td< td=""><td>K HK</td></td<>  | K HK  |
| 24       III       II       IV       17 05       13 23         23       III       IV       I       13 23       II       IV       13 07 18         22       II       IV       V       15 12 20       AH BK D       IV       IV         20       I       IV       III       03 24 26       AO BU CJ DA       IV       IV         19       II       I       III       22 04 24       AV BX FT GJ AV IU KT LV O       V         18       III       I       II       15 14 08       AV CI DO ES FK HY JT MA PW QX       VOH         17       I       V       IV       01 24 11       AL BQ DN EI FJ MY PW RX ST UZ       WDU         16       III       IV       II       16 23 17       AY BW CG DK EO FT HJ IX PQ UZ       EPH         14       V       III       I       11 15       AR DU EP GY IL JV KT MW NQ SX ZCM         13       IV       III       V       04 10 08       AL BD CN FY HX JS MR OT QU VZ       UMJ         12       V       IV       I       13 02 16       AG BH DW EK FQ IM LO PZ SV TU       YBM  | AX HI   |
| 23       III       IV       I       13       23         22       II       IV       V       13       07       18       IV         21       II       IV       V       15       12       20       AO       BU       CJ       DF         20       I       IV       III       O3       24       26       AO       BU       CJ       DF         19       II       I       III       22       O4       24       AV       FT       GJ       AV       IU       KT       IV         18       III       I       II       15       14       O8       AV       CI       DO       ES       FK       HY       JT       AOK         17       I       V       IV       01       24       11       AV       CF       DY       EU       GV       JO       KP       NS       RT       AOK         16       III       IV       I       04       07       15       AI       BQ       DN       EI       FJ       MY       PW       RS       ZC       MDU         15       IV       III       I       11  | LPE IG  |
| 22       II       IV       V       13       07       18       IV  | H HJN SE  |
| 20IIVIII032426AOBUCJDE19IIIIIIIII220424AVBXFVGJLVIUKTLVCV18IIIIII151408AVCIDOESFKHYJTMRPWQXVOH17IVIV012411AVCFDYEUGVJOKPNSRTAOK16IIIIVI040713ALBQDNEIFJMYPWRXSTUZWDU15IVIIII162317AYBWCGDKEOFTHJIXPQUZEPH14VIIII1115ARDUEPGYILJVKTMWNQSXZCM13IVIIIV041008ALBDCNFYHXJSMROTQUVZUMJ12VIVI130216AGBHDWEKFQIMLOPZSVTUYBM   | UP OEO XV   |
| 19IIIIII22 04 24AV BY F7 GJ LV IU KT LV OV18IIIIII15 14 08AV CI DO LS FK HY JT MR PW QXVOH17IVIV01 24 11AV CF DY EU GV JO KP NS RTAOK16IIIIVI04 07 13AL BQ DN EI FJ MY PW RX ST UZWDU15IVIIII16 23 17AY BW CG DK EO FT HJ IX PQ UZEPH14VIII11 11 15AR DU EP GY IL JV KT MW NQ SX ZCM13IVIIIV04 10 08AL BD CN FY HX JS MR OT QU VZUMJ12VIVI13 02 16AG BH DW EK FQ IM LO PZ SV TUYBM  | EFR VBW XI  |
| 18IIII151408AVCIDOESFKHYJFMKPWQXVOH17IVIV012411IIPWCFDYEUGVJOKPNSRTAOK16IIIIVI040713ALBQDNEIFJMYPWRXSTUZWDU15IVIIII162317AYBWCGDKEOFTHJIXPQUZEPH14VIIII1115ARDUEPGYILJVKTMWNQSXZCM13IVIIIV041008ALBDCNFYHXJSMROTQUVZUMJ12VIVI130216AGBHDWEKFQIMLOPZSVTUYBM  | LJA JBQ EH  |
| 17IVIVO1 24 11NEW CF DY EU GV JO KP NS RTAOK16IIIIVIO4 07 13AL BQ DN EI FJ MY PW RX ST UZWDU15IVIIII16 23 17AY BW CG DK EO FT HJ IX PQ UZEPH14VIIII11 11 15AR DU EP GY IL JV KT MW NQ SXZCM13IVIIIV04 10 08AL BD CN FY HX JS MR OT QU VZUMJ12VIVI13 02 16AG BH DW EK FQ IM LO PZ SV TUYBM   | PSZ GHZ CG<br>VXM JHM CT  |
| 16       III       IV       I       04       07       13       AL       BQ       DN       EI       FJ       MY       PW       RX       ST       UZ       WDU         15       IV       III       I       16       23       17       AY       BW       CG       DK       EO       FT       HJ       IX       PQ       UZ       EPH         14       V       III       I       11       15       AR       DU       EP       GY       IL       JV       KT       MW       NQ       SX       ZCM         13       IV       III       V       04       10       08       AL       BD       CN       FY       HX       JS       MR       OT       QU       VZ       UMJ         12       V       IV       I       13       02       16       AG       BH       DW       EK       FQ       IM       LO       PZ       SV       TU       YBM  | OOY IXN FO  |
| 15IVIIII162317AYBWCGDKEOFTHJIXPQUZEPH14VIIII111115ARDUEPGYILJVKTMWNQSXZCM13IVIIIV041008ALBDCNFYHXJSMROTQUVZUMJ12VIVI130216AGBHDWEKFQIMLOPZSVTUYBM   | URI KNA AQ  |
| 13IVIIIV041008ALBDCNFYHXJSMROTQUVZUMJ12VIVI130216AGBHDWEKFQIMLOPZSVTUYBM  | ICM ZHE QF  |
| 12 V IV I 13 02 16 AG BH DW EK FQ IM LO PZ SV TU YBM  | QZK VDA VJ  |
|   | JXO WPG VS  |
| IN THE LAND AND THE REAL THE AND THE AND THE REAL THE AND THE | EAX CDW BN<br>EIX RXZ XG  |
|   | AVR VXX HJ  |
|   | ABQ MBD YG  |
| 08 III IV V 05 26 06 BE CI DU FK GM HV JR LO NZ QY JZV  | WXL MZK KE  |
| O7 I IV V O4 O1 O8 BUCE DS GX IV KL MT NW OP QZ OTG   | LWG WMI HO  |
|   | VSD NRQ II  |
|   | OAQ PHM KW  |
|   | the second se |
| OZ II I III 24 OZ 21 AY BZ CQ EX FJ GI KW MS NP RT HAS  | QEW VDZ UG<br>KBO RLF IW  |



#### Enigma Cryptanalysis

- In December 1932, Marian Rejewski, polish mathematician and cryptanalyst, was able to break the Enigma cipher by using the theory of permutations.
- Later he and his fellow cryptanalysts continued on improving there methods and invented devices, such as the Bomba, to aid their efforts.
- The poles initiated the British and French military intelligence about the enigma and their decryption techniques and equipment.

#### Enigma Cryptanalysis

- During the war British cryptanalysts, most notably in blackly park, decrypted a vast number of messages enciphered on Enigma.
- Most notably the cryptanalysts at Bletchley park, most famous Alan Turning, improved upon the existing methods and were able to break into messages in less then 24 hours.

# Modern Cryptography

# Modern cryptography

- With the advent of computers, classic ciphers became impractical.
- As the computation power allowed swift and effective attacks against even the strongest of classic pen and paper ciphers.
- Higher standards are required for crypto-systems to be viable.
- So newer methods were developed using computers.

## "The Enemy knows the system"

**Claude Shannon** 

#### Modern cryptography Theoretical beginnings

- In 1948, Claude E. Shannon published the paper *A Mathematical Theory of Communication*, which is seen as the foundation of modern information theory.
- Shannon defined the concept of **perfect secrecy**. A cipher with such a property produces ciphertext that has no statistical relation to the plaintext.
- An example of a cipher with perfect secrecy is **One-time pad**.

#### **One-Time Pad** Unbreakable encryption

- First described by banker Frank Miller in 1882.
- The keys must be truly <u>random</u>.
- And at least the length of the plaintext.
- The function is identical to the simple Vigenère cipher with a infinite and random key.
- Has perfect secrecy.





 58653
 05891
 77973
 79940
 17490
 39253
 24941
 53184
 40837
 93714

 11454
 03055
 15565
 17466
 26950
 54906
 79183
 **59860 19381 19381 19381 19381** 79839
 34262
 02507
 83710
 37437
 47593
 63565
 17439
 06854
 81022

 73745
 65915
 79915
 35814
 63947
 24435
 44379
 74067
 44737
 12403



#### **One-Time Pad** Cryptanalysis

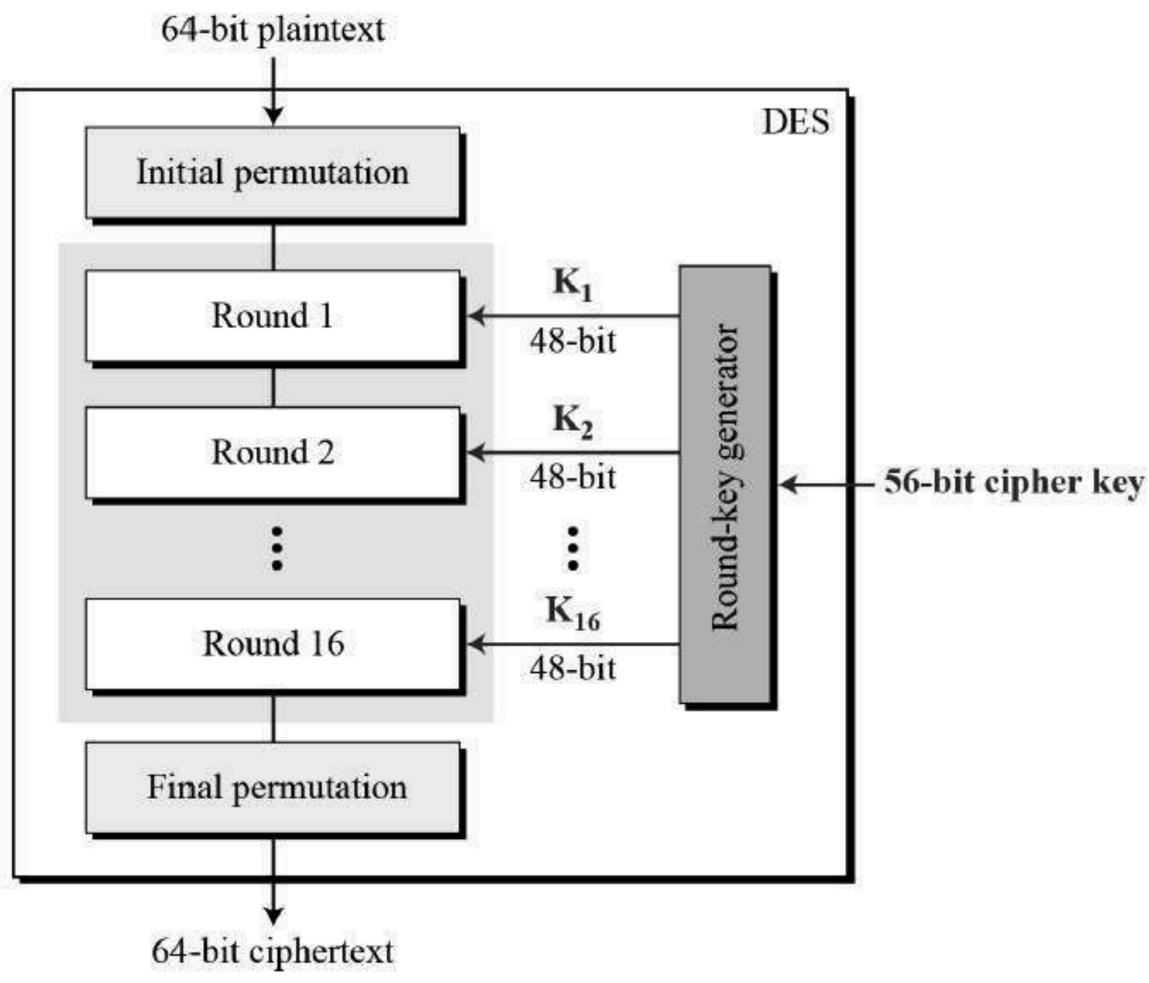
- It is truly unbreakable, if it is properly used.
- same key requirements.
- The key requirements make it very cumbersome to use.

• It is mathematically proven that any cipher to have perfect secrecy must have the

### DES

#### **Data Encryption Standard**

- Commissioned by the NSA and developed by IBM in 1972.
- One of the first publicly available modern crypto system that saw wide usage.
- It Is an implementation of a Feistel Cipher.





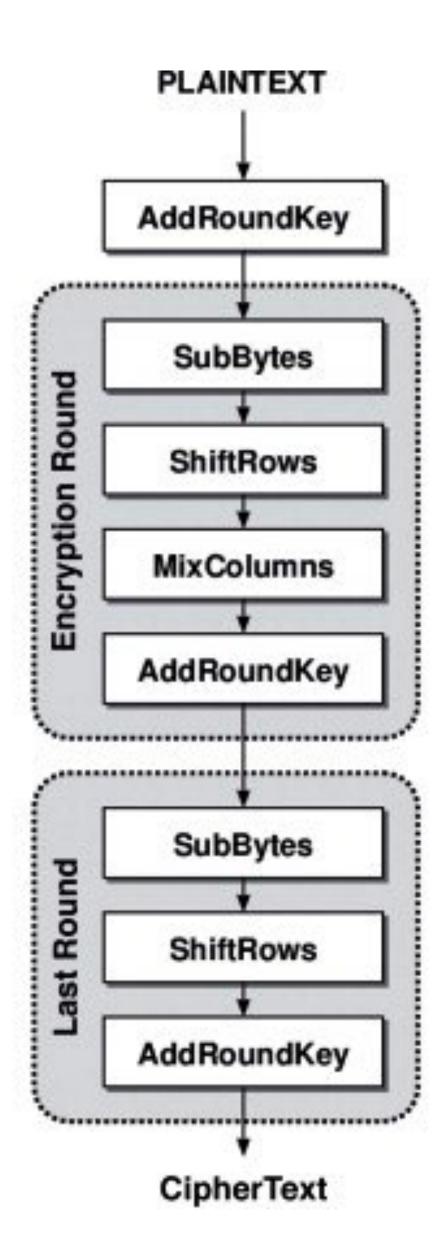
#### **DES** Cryptanalysis

- Although a powerful cipher, many were concerned over its implementation.
- The short key length of 56-bits, and NSAs involvement in the development as such changing the original setting of the S-Boxes.
- Although the suspicions over the weakness of the S-Boxes were relieved, as in 1990 Eli Biham and Adi Shamir independently developed **differential cryptanalysis**, and in a published paper found out that DES S-Boxes are much more resistant then if they were chosen at random.
- In the end the short key size made the cipher insecure against brute force attacks.

### AES

#### **AKA Rijndael**

- Developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.
- Originally called Rijndael.
- Proposed to NIST as a replace DES.
- It was accepted as the AES in 2001.



#### AES Cryptanalysis

- AES is based on substitution-permutation network design.
- It supports key lengths of 128, 192 and 256 bits.
- The calculations are done in the finite field GF(2) with the given irreducible polynomial  $x^8 + x^4 + x^3 + x + 1$ .
- No practical attacks have been found until now, and it is considered secure for the long term.
- This is by far the most widely used cipher, and it is embedded both into computer software and hardware.

### Fundamentalissues

- What we have described so far is called **Symmetric-key Cryptography**; Both parties must possess the same key.
- The key distribution problem is a fundamental, and the systems in place for solving it can be very complex and error prone.
- So far there is no way to determine that the validity of the messages.

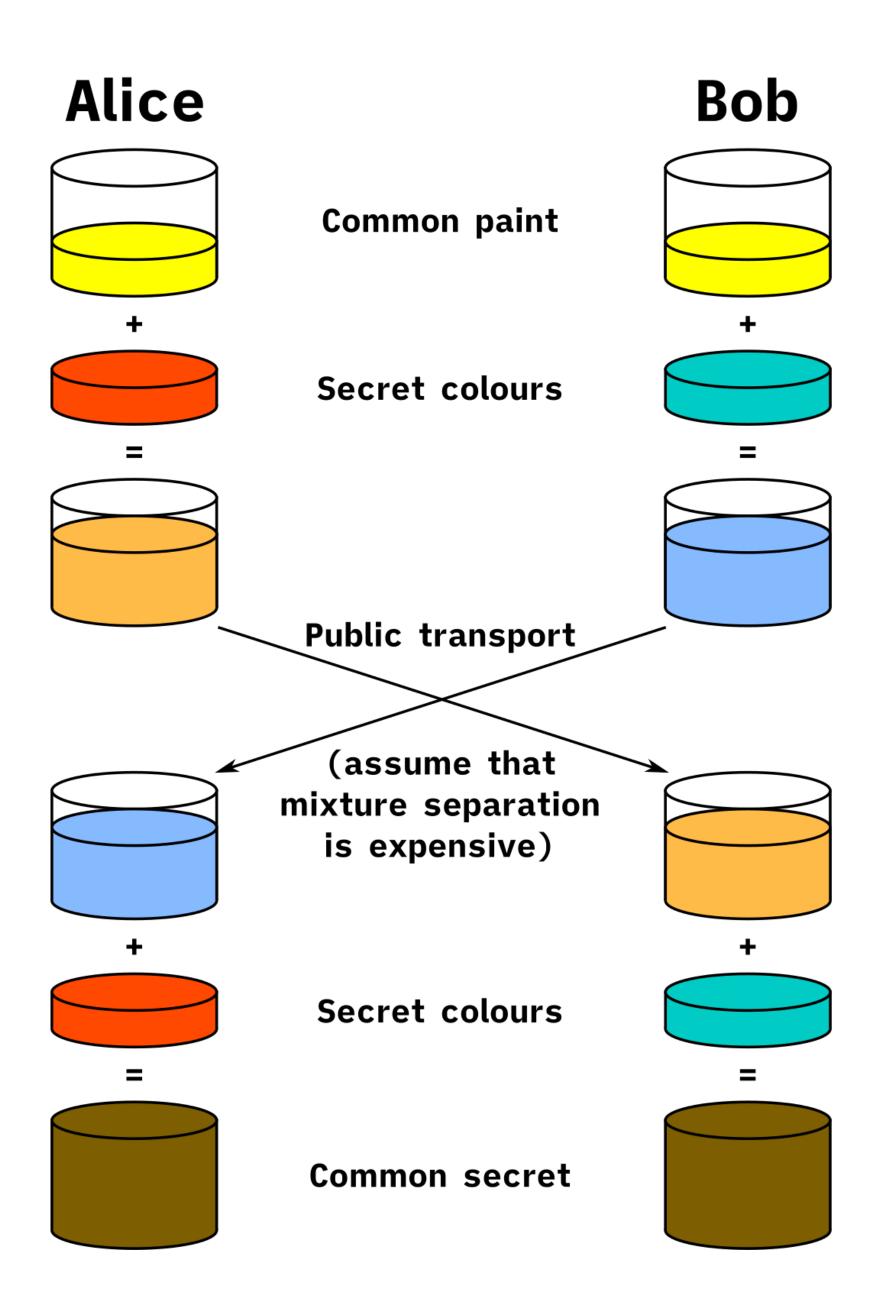
Public-Key Cryptography

# Public-Key Cryptography

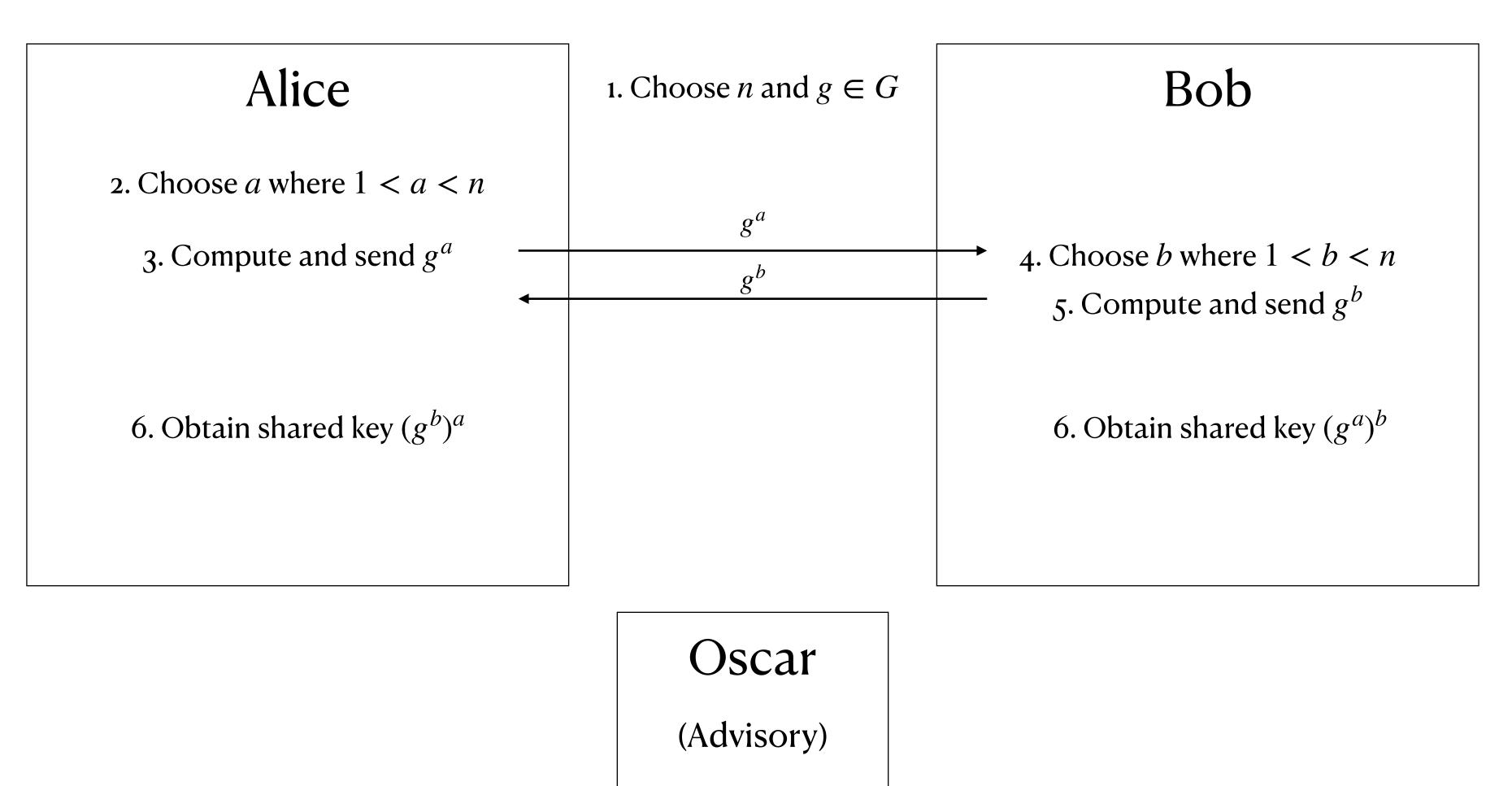
- Whitfield. Diffie And Martin E. Hellman published *New directions in Cryptography* in the year 1976, in which they proposed a way of doing cryptography.
- In it they proposed public key cryptography.
- Solved both issues of key distribution problem and a proposed way of doing identity validation (**digital signatures**).
- The key idea is to separate encryption and decryption keys to a **public key** and a **private key**.

#### Diffie-Hellman Key Exchange

- First conceived by Ralph Merkle, published in the same paper.
- Solves the key distribution problem.
- Should be paired with symmetric key systems.



#### Diffie-Hellman Key Exchange Algorithm



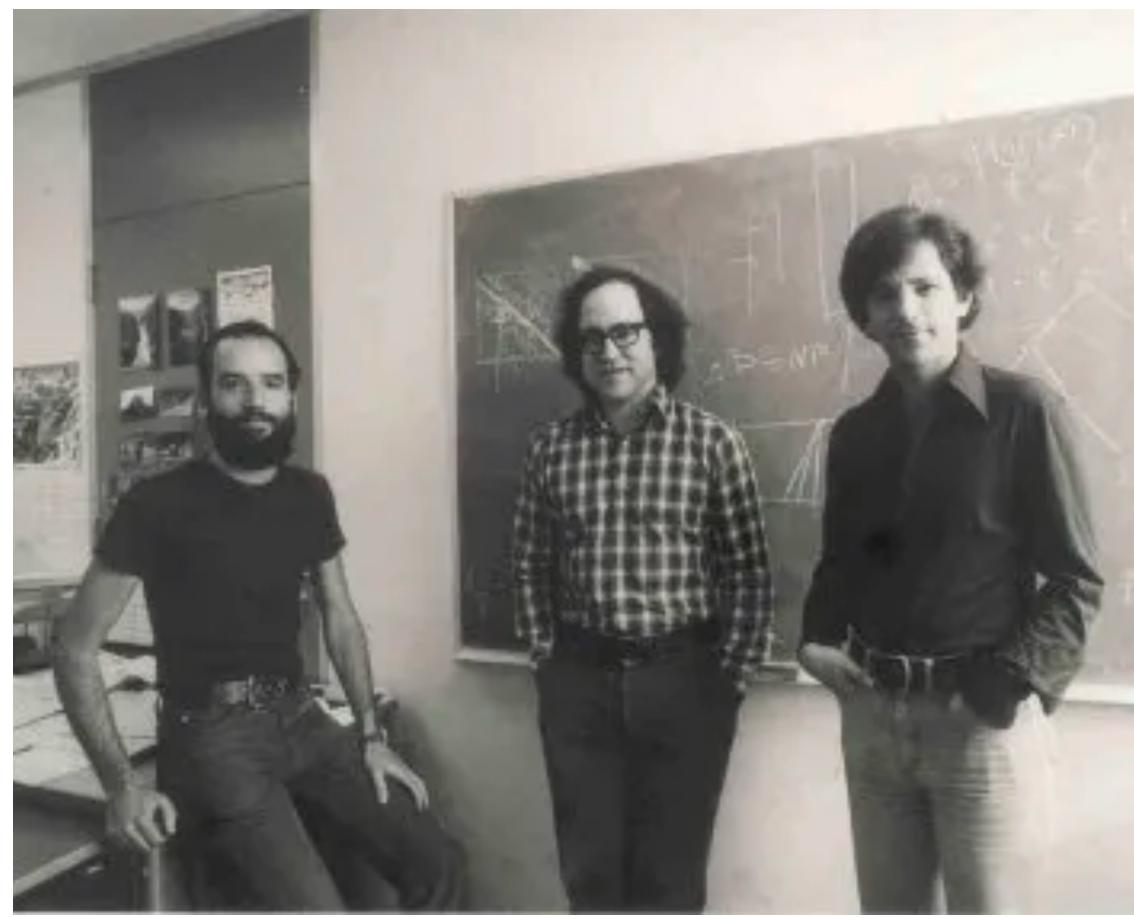
### Diffie-Hellman Key Exchange Cryptanalysis

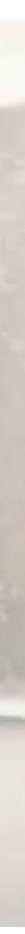
- The security of this crypto-system is based on the fact that even with the knowledge of  $g^{ab}$ ,  $g^{a}$ , and  $g^{b}$  there is no effective algorithm to compute the private key exponents *a* or *b*.
- We can generalise this to the **Discrete Logarithm Problem**. Let *G* be a cyclic group, and *g* a generator of *G*. Given  $h \in G$ , find the integer *t* such that  $g^t = h$ .
- In its most simple form G is multiplicative  $\mathbb{Z}_p$  where p is prime.

#### RSA

#### **Rivest - Shamir - Adleman**

- Developed in 1977.
- Uses integer factorisation as its security mechanism.
- Most commonly used public key crypto-system (Web, Banking, etc...)







- The key generation of RSA
  - 1. Choose two large primes p and q
  - 2. Compute n = pq
  - 3. Compute  $\phi(n) = (p-1)(q-1)$
  - 4. Choose *e* where  $2 < e < \phi(n)$  and  $gcd(m, \phi(n)) = 1$
  - 5. Compute  $d \equiv e^{-1} \mod \phi(n)$

The public key is (e, n) and private key d

#### RSA Algorithm

#### RSA Algorithm

# • Encryption and decryption are the following operations

- $E(m) = m^e \mod n$
- $D(c) = c^d = (m^e)^d = m \mod n$

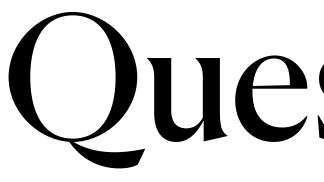
# Notes on group theory in Cryptography

# Notes on group theory in Cryptography

- Although number theory is mostly credited for cryptography, but also group theory has played a major role in the development of modern cryptographic system.
- As we saw before we can choose different platform groups for the key exchange protocol, such as group of points on an elliptic curve (elliptic curve cryptography).
- For non-abelian groups Conjugacy instead of exponentiation, such as using braid groups in Ko-Lee-Cheon-Han-Kang-Park. Or using the bracket operator (commutator) in Anshel-Anshel-Goldfeld, for any non-abelian group.
- But so far all of them have major drawbacks and a suitable platform group has yet to be found.

### References

- Understanding Cryptography, by Christof par.
- *Handbook of Applied Cryptography,* by Alfred Menezes, Paul van Oorschot, and Scott Vanstone.
- A Mathematical Theory of Communication, Claude shannon.
- New Directions in Cryptography. Whitfield. Diffie And Martin E. Hellman.
- Vist *dcode.fr* for interactive cryptography.



# Questions?