# CRYPTOGRAPHY & SOCIETY

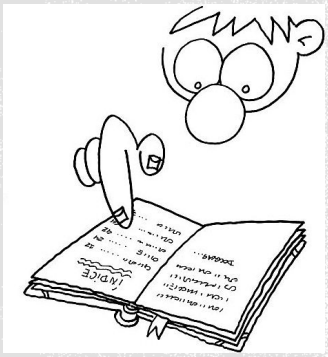
*Silvio Ranise* [ silvio.ranise@unitn.it or *ranise@fbk.eu* ]

UNIVERSITÀ DI TRENTO

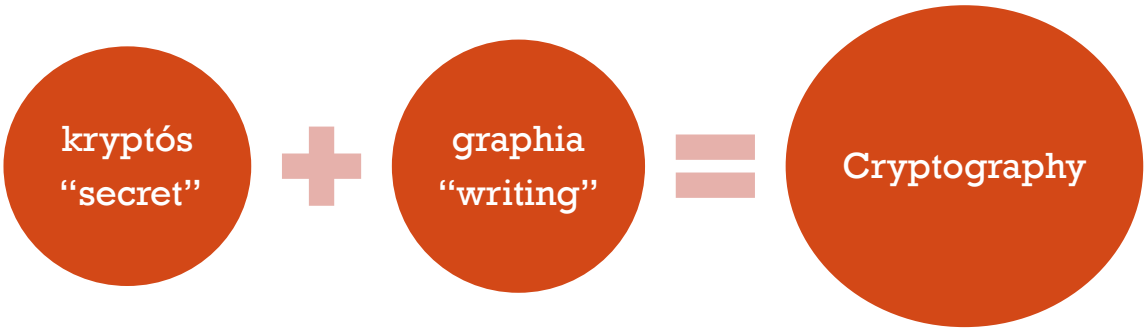
FONDAZIONE BRUNO KESSLER

## CONTENTS

- *Etimology*
- *History*: from Egypt to Roman Empire
- Caesar cipher
  - **QUESTION**: Key size and attack resistance
- *History*: Al-Kindi, Alberti and Vigenère
- Unbreakable ciphers: theory vs practice
  - **QUESTION**: Key distribution
- *History*: Modern cryptography after Turing
  - **On key size**: Symmetric key cryptography
  - **On key distribution**: Public key cryptography
- *Applications*
  - HTTP vs HTTPS
  - End to End Encryption
  - Client Side Scanning



# ETIMOLOGY




2

# 3 HISTORY

Partial and over-simplified

# HISTORY (1)

1900 BC

Add some mystery

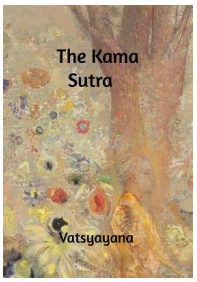
1500 BC

Protect recipe for pottery glaze

900 BC

Protect messages among troops

400 BC

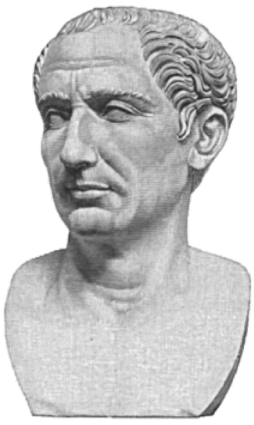



Protect messages between lovers

4

# HISTORY (2)

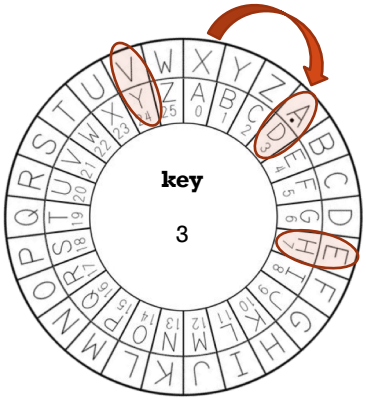
100 BC –44 BC



Protect messages of military significance

5

# DIGRESSION: CAESAR CIPHER (2)



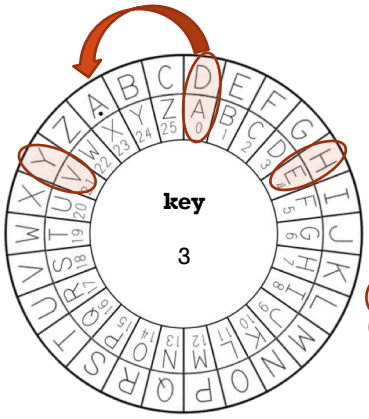

Plaintext: A V E

Encryption

Ciphertext: D Y H


6

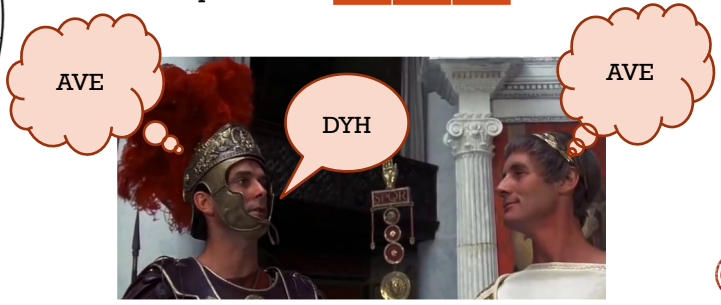
# DIGRESSION: CAESAR CIPHER (3)




Plaintext: D Y H

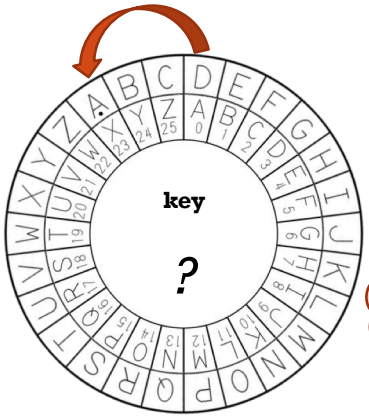
Decryption

Ciphertext: A V E




7

# DIGRESSION: CAESAR CIPHER (4)

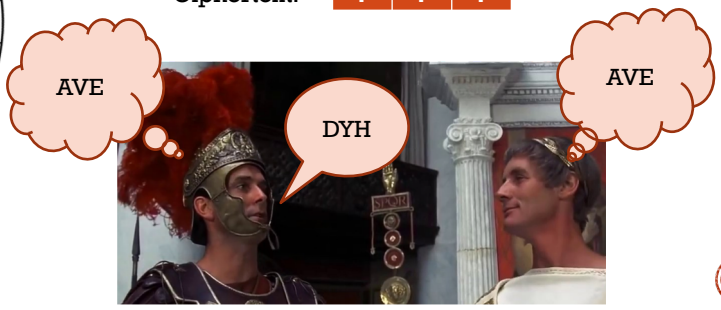



Attacker

Plaintext: D Y H

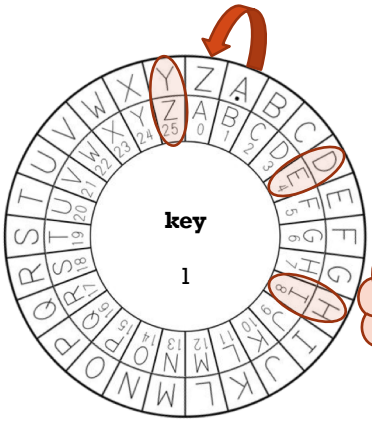
Decryption

Ciphertext: ? ? ?



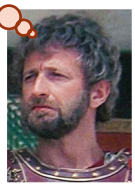

8

# DIGRESSION: CIPHER (6)




EZI

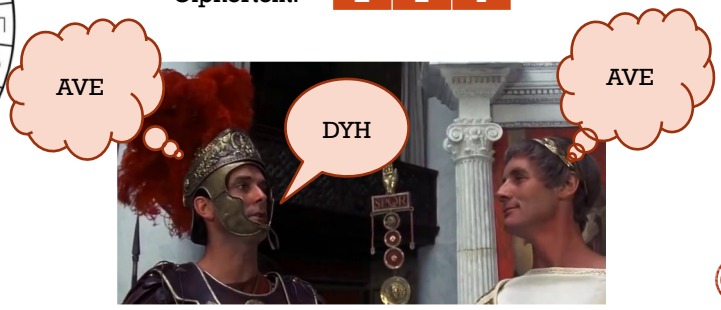
Attacker



Ciphertext: D Y H

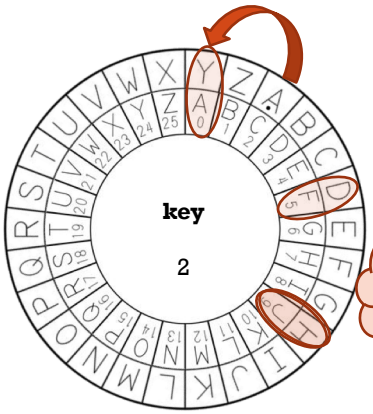
Decryption

Ciphertext: E Z I



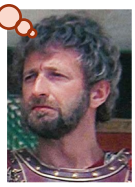

9

# DIGRESSION: CAESAR CIPHER (7)




FYJ

Attacker



Ciphertext: D Y H

Decryption

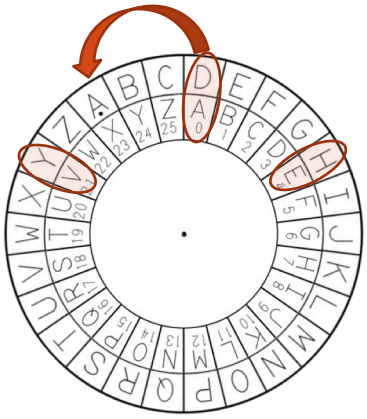
Plaintext: F Y J

AVE


AVE

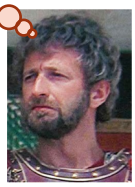
10

# DIGRESSION: CAESAR CIPHER (8)



AVE

Attacker



Ciphertext: D Y H

Decryption

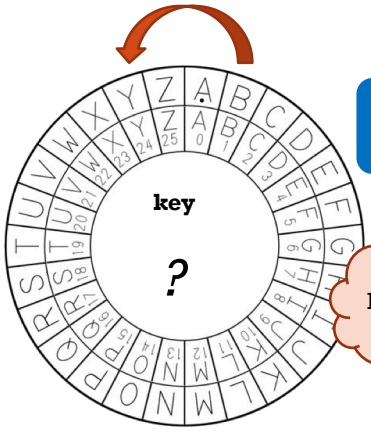
Plaintext: A V E

AVE


AVE

11

# DIGRESSION: CAESAR CIPHER (8)




How many attempts?

Ciphertext:

Decryption

Plaintext: ?

?

Attacker

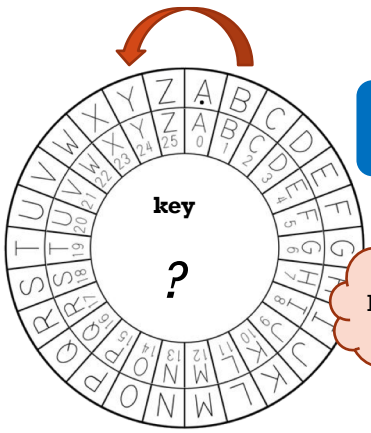
Plaintext

Ciphertext

Plaintext



# DIGRESSION: CAESAR CIPHER (9)




How many attempts?

25

Ciphertext:

Decryption

Plaintext: ?

?

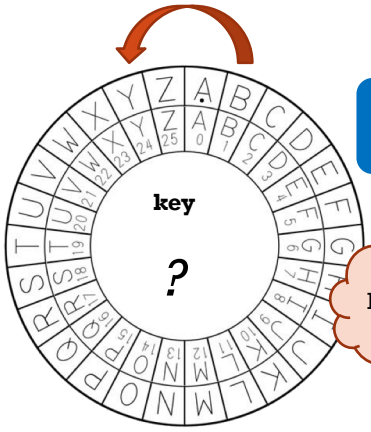
Attacker

Plaintext

Ciphertext

Plaintext

# DIGRESSION: CAESAR CIPHER (10)



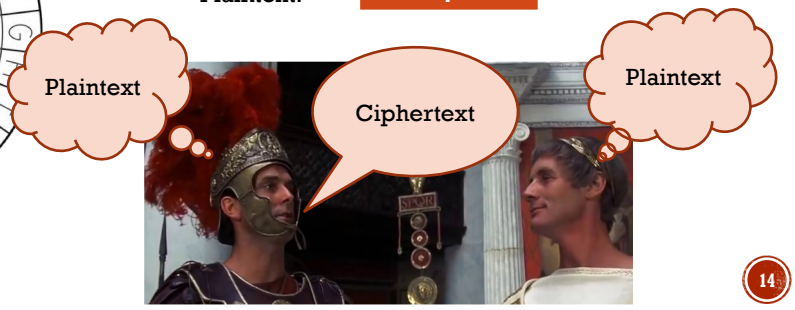

Ciphertext:

How long does it take?

Few minutes by hand

Decryption

Plaintext: ?


14

15

# HOW MANY KEYS FOR A CIPHER TO BE CONSIDERED SECURE IN PRESENCE OF MODERN COMPUTERS?

Please, remember this question!

16

# HISTORY CONTINUED

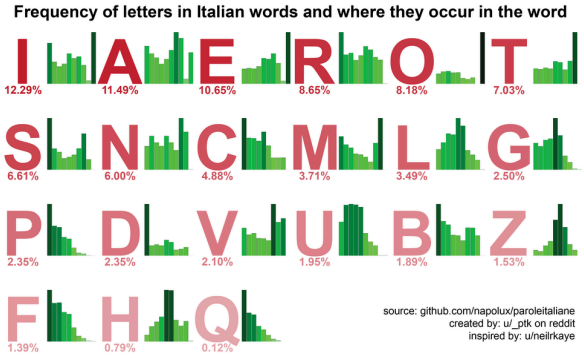
Partial and over-simplified

# HISTORY (3)

850 AC

The birth of cryptanalysis

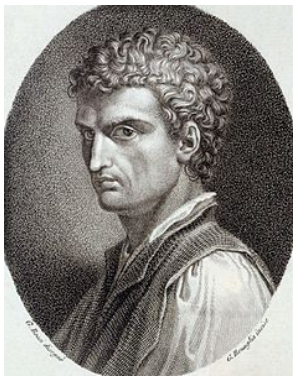
Al-Kindi



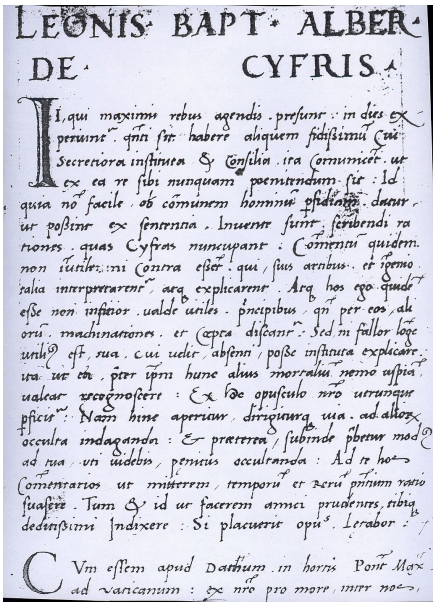

17

# HISTORY (4)

1406 –1472



Leon Battista Alberti
Father of Western cryptography



LEONIS BAPT. ALBER-
DE CYFRIS.

I, qui maximis rebus agendis præsunt : in dies ex
primis quæ sit habere aliquem fidissimum Cui
Secretiora instituta & consilia ita communicet ut
ex ea re sibi nunquam pœnitendum sit : Id
quia no facile ob communem hominu ofdiam. datur
ut postint ex sententia, Inuenit sunt scribendi ra
tiones quas Cyfras nuncupant : Commodi quidem
non inutiles, ni contra esset qui suis armis et remo
ralia interpretarent, arq explicarent. Arq hos ego quide
esse non inficior ualde utiles præcipibus qn per eos alio
rum machinationes et cœpta discant : Sed ni fallor hoc
unu est, sua cui uelit absenti posse institura explicare
ita ut eo per ipm hunc alius mortaliu nemo ussus
ualeat recognoscere : Ex hoc opusculo nro utrunque
pstitit : Nam hinc aperiur disciplina qua ad alios
occulta indagando : & præterea subinde pbeum mod
ad qua uti uelis, penitus occultanda : Ad te hoc
Comentarios ut mittrem, temporu et rerum rationi
suasere. Tum & id ut facerem amici prudentes, tibiq
dedissimi indixere : Si placuerit opus. Ierabor :

Cum essem apud Datium in horti Pont Max
ad Vaticanum : ex nro pro more mitt noc-



# HISTORY (5)

It was already invented by Alberti!

1523–1596

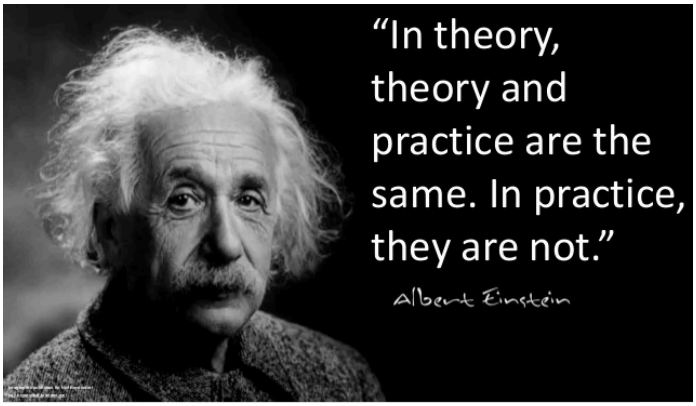
Blaise de Vigenère


**Perfect / indecipherable** cipher

It can be seen as a series of Caesar ciphers defined by a key

# DIGRESSION: SO, PROBLEM SOLVED!?!?!?

| | THEORY | PRACTICE |
|---|---|---|
| **Answer** | YES | NO |



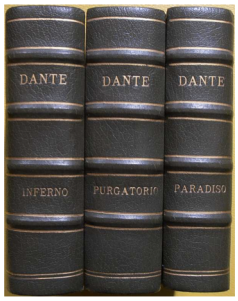

20

# DIGRESSION: SO, PROBLEM SOLVED!?!?!?

| | THEORY | PRACTICE |
|---|---|---|
| **Answer** | YES | NO |

Notice that Vigenère cipher is **perfect** with a **key** of the **same length of the message** being encrypted

Plaintext




21

# DIGRESSION: SO, PROBLEM SOLVED!?!?!?

| | THEORY | PRACTICE |
|---|---|---|
| **Answer** | YES | NO |

Notice that Vigenère cipher is **perfect** with a **key** of the **same length of the message** being encrypted

Plaintext + Key = Ciphertext

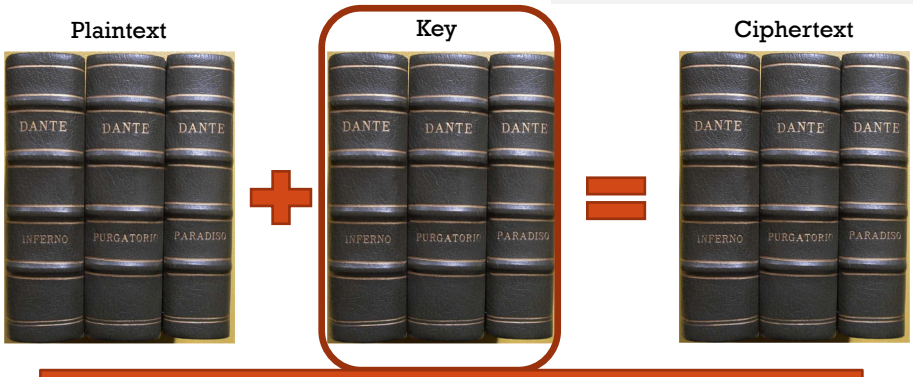

22

# DIGRESSION: SO, PROBLEM SOLVED!?!?!?

| | THEORY | PRACTICE |
|---|---|---|
| **Answer** | YES | NO |

Notice that Vigenère cipher is **perfect** with a **key** of the **same length of the message** being encrypted

Plaintext + Key = Ciphertext




How do you securely exchange the key between sender and receiver?

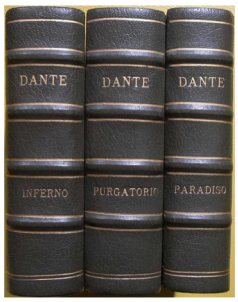
23

# DIGRESSION: SO, PROBLEM SOLVED!?!?!?

| | THEORY | PRACTICE |
|---|---|---|
| **Answer** | YES | NO |

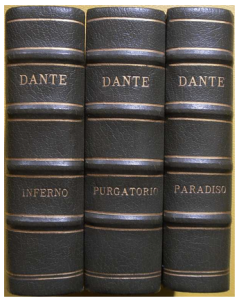
Notice that Vi[illegible]her is **perfect** with a **key** of th[illegible] **length of the message** bei[illegible]ted

Plaintext




key

Ciphertext




In practice, we consider only approximations of Vigenère cipher with small keys that are easier to distribute!

24

25

# HOW CAN WE SECURELY DISTRIBUTE KEYS WHEN ENTITIES ARE GEOGRAPHICALLY DISTRIBUTED?

Please, remember this question!

26

# HISTORY CONTINUED, AGAIN

Partial and over-simplified

## HISTORY (6)

- From here on, most of the cryptographic techniques attempt to
  - approximate as much as possible Vigenère cipher
  - find clever ways to exchange keys in secure ways
- Indeed, **I am cheating**
- It is a dramatic over-simplification but still useful for this presentation…

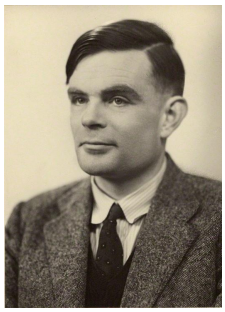
27

# HISTORY (7)

https://themobilityforum.net/2020/06/11/enigma-code-innovation-that-saved-14-million-lives/#:~:text=It%20is%20estimated%20that%20Turing's,and%20saved%2014%20million%20lives

- The *enigma* machine was used to secure communication of German military throughout the 2nd World War …
- … its cryptanalysis changed the course of human history
- Estimated that it
  - **shortened the war of 2 years**
  - **saved 14 million lives**

Dramatic impact!



Alan Turing

28

29

# HOW MANY KEYS FOR A CIPHER TO BE CONSIDERED SECURE IN PRESENCE OF MODERN COMPUTERS?

Again…

# FROM CLASSIC TO MODERN CRYPTO (1)

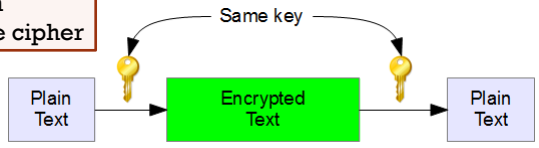
- With the development of the computer (**after Alain Turing pioneering work on characterizing computation**), it become difficult to depend on the elementary classical techniques as it is easy to decrypt the ciphertext
  - Caesar cipher can be brute forced in 25 attempts in the worst case!
  - This can be done instantly with a computer

- With the development of **computer networks**, distributing keys among geographically distributed users is getting more and more difficult

# FROM CLASSIC TO MODERN CRYPTO (2)

**Symmetric** key cryptography

Based on Vigenère cipher




| Pros | Cons |
|---|---|
| Fast | Key distr |

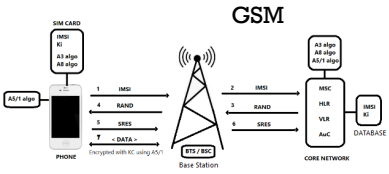
**Public** key cryptography

Based on a variety of problems in number theory

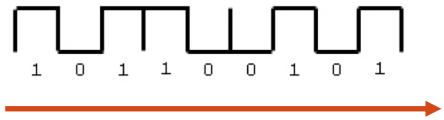

| Pros | Cons |
|---|---|
| Key distr | Slow |

# FROM CLASSIC TO MODERN CRYPTO (3)

Symmetric ciphers: **stream**




Bluetooth®

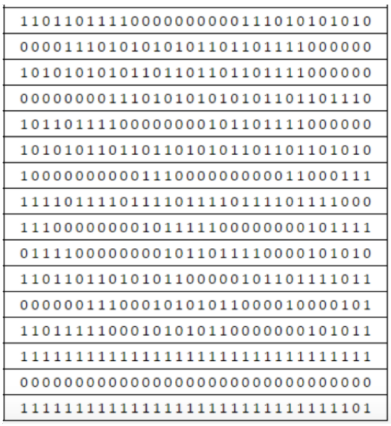



32

# FROM CLASSIC TO MODERN CRYPTO (4)

Symmetric ciphers: **block**

- *Data Encryption Standard (DES)*
- Designed by IBM in 1970
- Adopted as a standard in 1977
- **Key size: 56 bits**
- Withdrawn in 2005 because shown to be weak…




33

# DIGRESSION: NUMBER OF KEYS

| Key size (bits) | Number of keys |
|---|---|
| 1 | 2 |
| 2 | 2*2=4 |
| 3 | 2*2*2=8 |
| 4 | 2*2*2*2=16 |
| 5 | 2*2*2*2*2=32 |
| 6 | 2*2*2*2*2*2=64 |
| 7 | 2*2*2*2*2*2*2=128 |
| … | … |

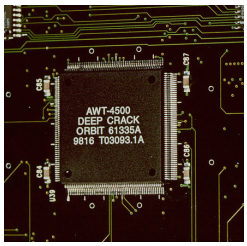
- DES key size = 56 bits
- DES number of keys = $2^{56}$ = 72,057,594,037,927,936 ≈ $7 * 10^{16}$

34

# DIGRESSION: CRACKING DES (1998-1999)

CRYPTOGRAPHY RESEARCH
Advanced Wireless Technologies
ELECTRONIC FRONTIER FOUNDATION EFF

**Deep crack chip**
(especially designed
for the purpose of cracking DES)




Deep crack consisted of 1,856 Deep crack chips + PC
for a cost of only 250,000 $

- Deep crack was able to test **90 billion keys per second**
- It was able to **crack** a DES **key** in **less than a day**!

DES was no more considered as a standard in 2001…

35

# FROM CLASSIC TO MODERN CRYPTO (5)

- In 1997, NIST initiated a public, 4-1/2 year process to develop a new secure cryptosystem for U.S. government applications (as opposed to the closed process in the adoption of DES 25 years earlier)
- Result was the Advanced Encryption Standard (**AES**) that became the official successor to DES in December 2001
- AES uses a symmetric key crypto scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen
- **The algorithm can use a variable key size of 128, 192, or 256**

Learning from previous errors…

36

# DIGRESSION: DES VS AES & THE FUTURE…

- In DES, there are approximately
  - $7.2 \times 10^{16}$ possible DES keys
- In AES, there are approximately:
  - $3.4 \times 10^{38}$ possible 128-bit keys
  - $6.2 \times 10^{57}$ possible 192-bit keys
  - $1.1 \times 10^{77}$ possible 256-bit keys

There are around **$10^{21}$ times more AES 128-bit keys than DES 56-bit keys**

- NIST's DES was a U.S. government standard for approximately 20 years before it became practical to mount a brute force attack with specialized hardware
- The AES supports significantly larger key sizes than what DES supports
- AES has the potential to remain secure well beyond 20/30 years

We are still left with a big problem…

37

38

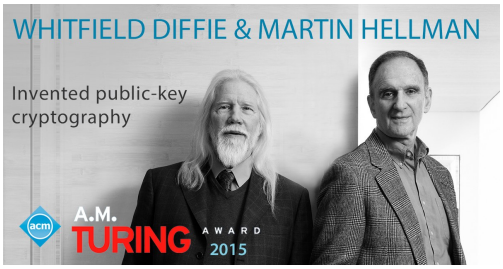
# HOW CAN WE SECURELY DISTRIBUTE KEYS WHEN ENTITIES ARE GEOGRAPHICALLY DISTRIBUTED?

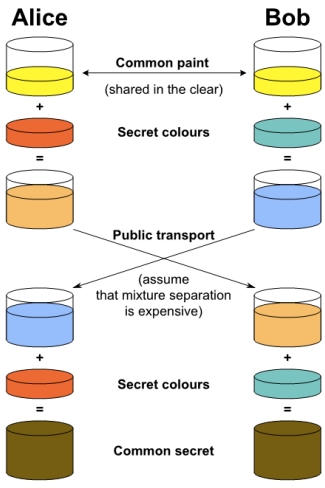
Additional question!

# FROM CLASSIC TO MODERN CRYPTO (6)

Public key cryptography: **Diffie-Hellman**

- 1976: most significant result in cryptography in the last 300-400 year
- Secure key distribution over insecure channel



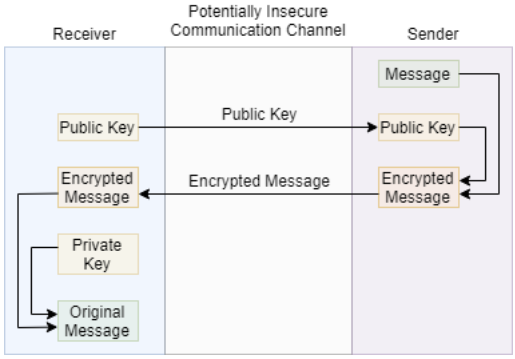




39

# FROM CLASSIC TO MODERN CRYPTO (7)

Public key cryptography: **RSA**

- 1977: **used in almost all Internet-based commercial transactions**
- Not only secure key distribution over insecure channel

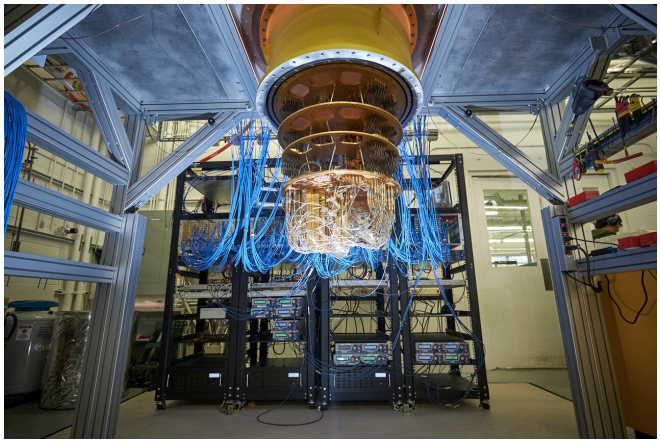

40

41

# A COMBINATION OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY IS UBIQUITOUSLY USED TO SECURE TRANSACTIONS OVER THE INTERNET

# DIGRESSION: WHAT ABOUT QUANTUM?

- **How secure is public key cryptography?**
- Unbreakable for classical computer (provided adequate key size is used)…
- … no more so with quantum computers (regardless of the key size)!
- Quantum computers will be ready in 10 year (or even more)…
- So, why worrying now for developing new cryptographic primitives to protect electronic transactions?



https://phys.org/news/2020-08-google-largest-chemical-simulation-quantum.html

42

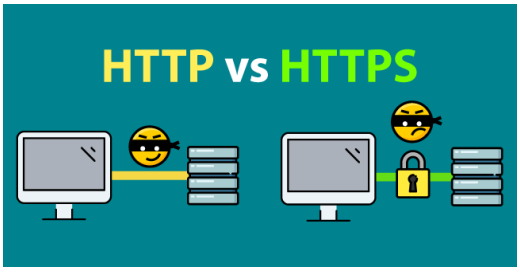
# FROM CLASSIC TO MODERN CRYPTO (8)

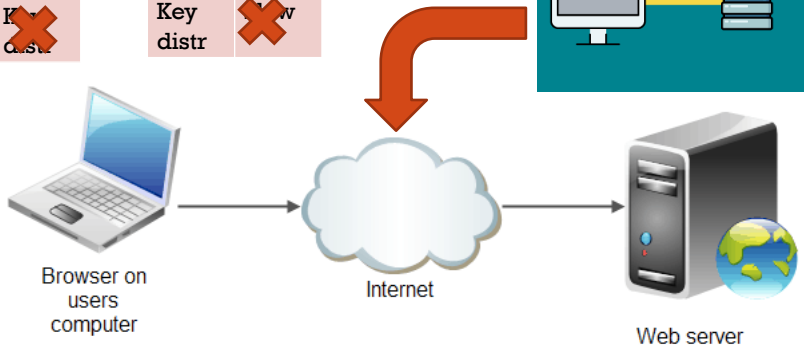
Protocol combining

Symmetric and Public key cryptography

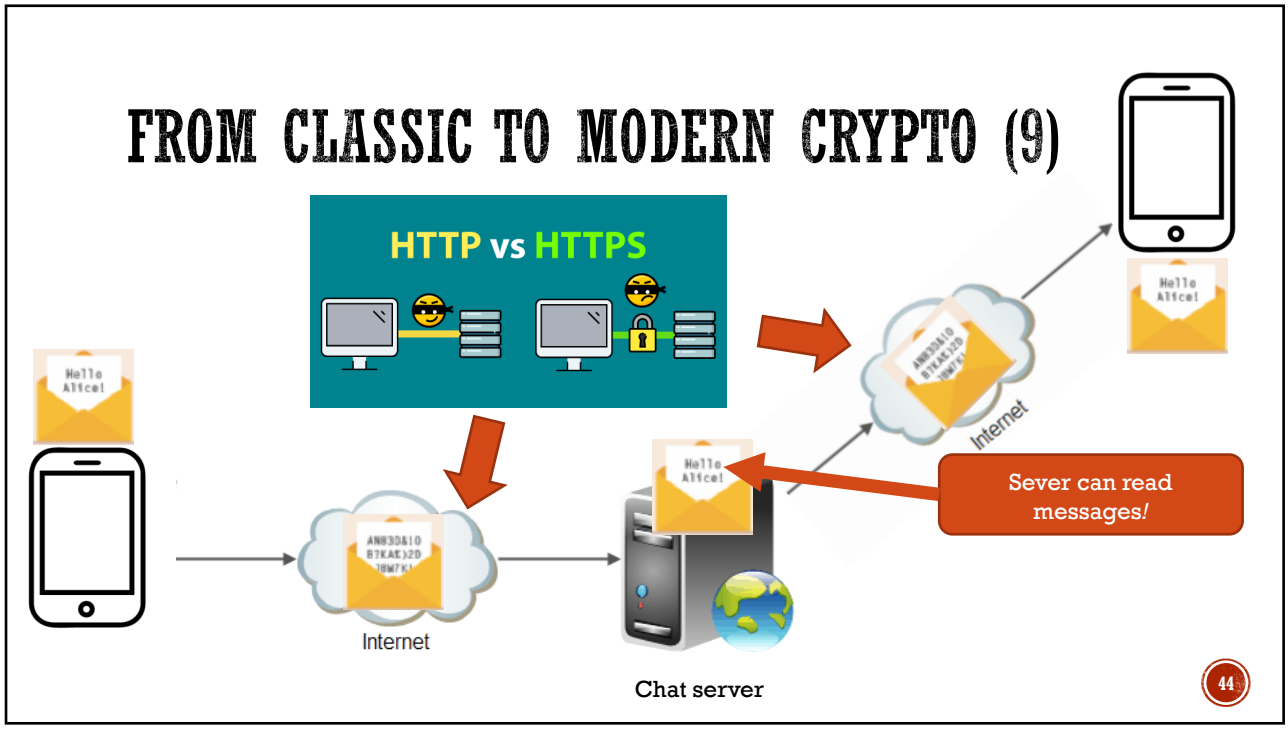
| Pros | Cons |
|---|---|
| Fast | K… c… |

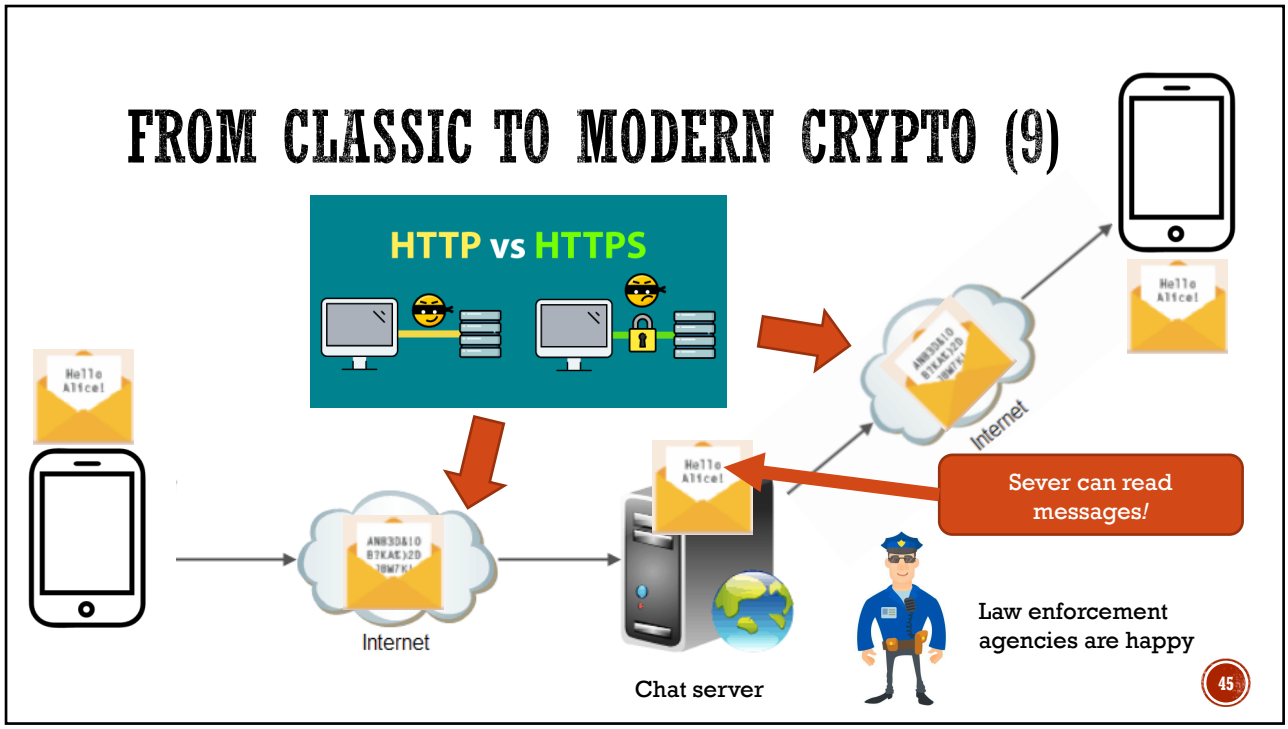
| Pros | Cons |
|---|---|
| Key distr | … |




43


FROM CLASSIC TO MODERN CRYPTO (9)
HTTP vs HTTPS
Internet
Sever can read messages!
Chat server
44


FROM CLASSIC TO MODERN CRYPTO (9)
HTTP vs HTTPS
Internet
Sever can read messages!
Law enforcement agencies are happy
Chat server
45

# FROM CLASSIC TO MODERN CRYPTO (10)




# FROM CLASSIC TO MODERN CRYPTO (10)


Law enforcement agencies are much less happy

# FROM CLASSIC TO MODERN CRYPTO (10)


Law enforcement agencies are much less happy

48

# LEA ASK FOR BACKDOORS


https://twitter.com/PrivacyCamp/status/701030778541572096/photo/1

49

https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf

# APPLE RECENTLY PROVIDES AN ALTERNATIVE: CLIENT SIDE SCANNING (CSS)

**GOAL**
Child sexual abuse material detection

CSS can read messages!


Sever cannot read messages!

Law enforcement agencies are happy again!

S. Ranise - Security & Trust (FBK)

50

# CSS PROBLEMS (1)

Plus several other technical problems such as violation of Principle of least privilege…

False positives!

https://techxplore.com/news/2021-10-client-side-scanning-bugs-pockets.html

51

# CSS PROBLEMS (2)

Potential for abuse!

- Who can guarantee that the **scope of application** is only the prevention of child sexual abuse?
  - Europe suggested to include any kind of sexual abuse plus terrorism…
- **Where** should we **stop enlarging the scope of applicability**?
  - Answering this question is fundamental to **democracy**…
    - Think of large scale censorship…
  - What about **non democratic regimes**?
    - Think of minorities…

Many more details in the following report
https://arxiv.org/pdf/2110.07450.pdf


https://blog.cryptographyengineering.com/