Informatica II (Laboratorio)

Corso di laurea magistrale in Scienze pedagogiche

Introduzione alla sicurezza informatica (cybersecurity)

Andrea Bracciali – a.a. 2024/2025

These slides have been developed by the contribution of prof. Giovanni Quattrone

In this lesson

- Information security

Information security

- Security → *keeping the information safe*
- Early ages: isolated room
- Today?
  - We are globally connected.
  - This is a threat to our security.
- Vulnerable spots
  - Home → Door, windows
  - Computer science → ?

Hackers and Crakers

- Hackers... in the origins
  - Computer enthusiasts
  - Thinkers
  - Fixers
- Hackers... today
  - Negative meaning.
- Crakers
  - Break into someone else's computer

Be aware!

Any time of hacking is illegal!

Authentication

Login:

Password:

Authentication

Login: Alice

Password: * * *

Authentication

Login: Alice

Password: fox

Login	Password
Alice	fox
John	car
Louis	red

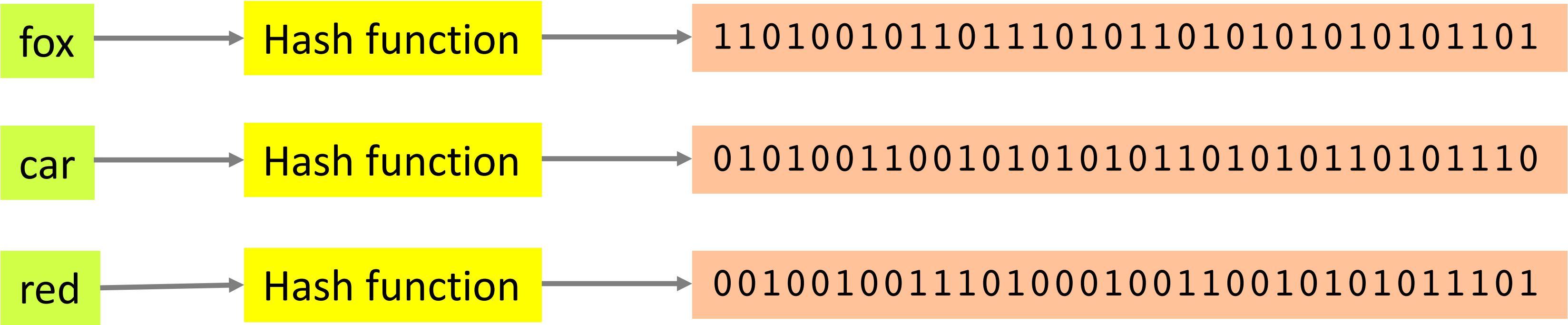
Issues?

Easy to attack

Authentication

Login:

Password:



fox → Hash function → 1101001011011101011010101010101101

car → Hash function → 0101001100101010101101010110101110

red → Hash function → 0010010011101000100110010101011101

Authentication

Login: Alice

Password: fox

Login	Password
Alice	1101001011011101011010101010101101
John	0101001100101010101101010110101110
Louis	0010010011101000100110010101011101

Authentication

- Attacks
  - Brute force

Login	Password
Alice	a
Alice	b
Alice	c
…	…
Alice	aa
Alice	ab
Alice	ac
…	…
Alice	aaa
Alice	aab
Alice	aac
…	…

Authentication

- Defenses
  - Always use a strong password (Longer than 8 characters, containing letters, numbers, special characters)
  - Use different passwords in different systems
  - Do not use your day of birth and other trivial passwords

hello	weak password
ae!RTr4=-2Xdg	strong password

Two-Factor Authentication

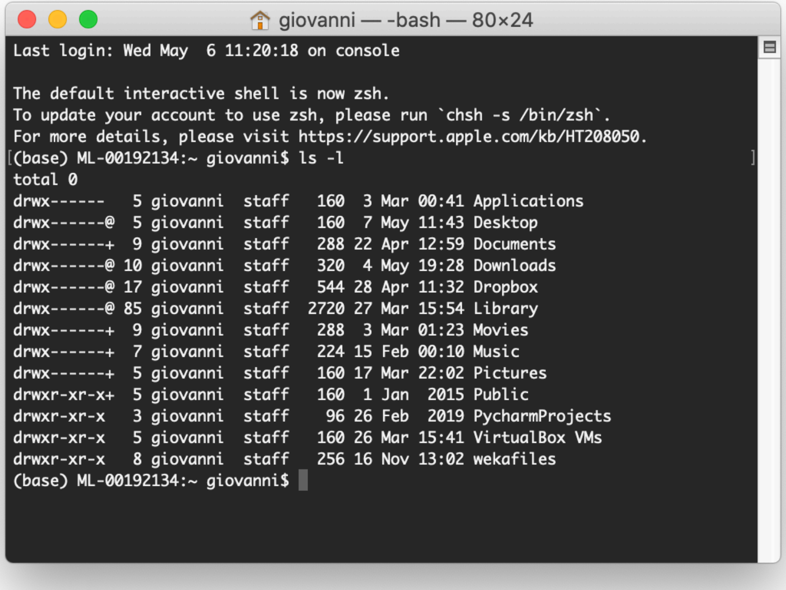
Login: Alice

Password: * * *

PASSWORD
VERIFY
Username
****
Login

Authorization

- Read access
- Write access
- Execute access
- Delete access



```
Last login: Wed May  6 11:20:18 on console

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
(base) ML-00192134:~ giovanni$ ls -l
total 0
drwx------   5 giovanni  staff   160  3 Mar 00:41 Applications
drwx------@  5 giovanni  staff   160  7 May 11:43 Desktop
drwx------+  9 giovanni  staff   288 22 Apr 12:59 Documents
drwx------@ 10 giovanni  staff   320  4 May 19:28 Downloads
drwx------@ 17 giovanni  staff   544 28 Apr 11:32 Dropbox
drwx------@ 85 giovanni  staff  2720 27 Mar 15:54 Library
drwx------+  9 giovanni  staff   288  3 Mar 01:23 Movies
drwx------+  7 giovanni  staff   224 15 Feb 00:10 Music
drwx------+  5 giovanni  staff   160 17 Mar 22:02 Pictures
drwxr-xr-x+  5 giovanni  staff   160  1 Jan  2015 Public
drwxr-xr-x   3 giovanni  staff    96 26 Feb  2019 PycharmProjects
drwxr-xr-x   5 giovanni  staff   160 26 Mar 15:41 VirtualBox VMs
drwxr-xr-x   8 giovanni  staff   256 16 Nov 13:02 wekafiles
(base) ML-00192134:~ giovanni$ 
```

Threats from the Network

- Virus
- Worm
- A Trojan horse

Cosa sono?

p.381 del libro (per una possibile definizione)

Defense

- Up-to-date antivirus
- Up-to-date firewall
- Latest security patches
- Don’t open e-mail attachments from unknown sources
- Don’t download software except from reputable sources
- Don’t send personal or financial information in response to any e-mail

Phishing

Phishing is a practice used to illegally obtain sensitive information such as credit card numbers, account numbers, and passwords.

The Anti-Phishing Working Group (APWG) is an industry and law enforcement association focusing on helping eliminate identity theft resulting from phishing (www.antiphishing.org/index.html).

The term "phishing" comes about
because perpetrators cast out bait,
in the form of e-mail messages,
to thou- sands of potential victims
in the hope that one or two will "bite"
and fall for this scam.

Encryption

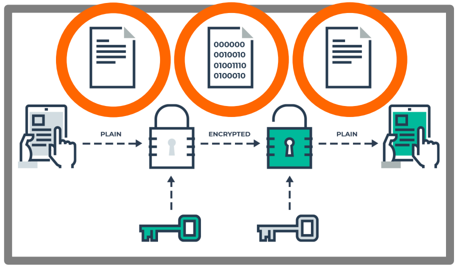
- Most of today’s corporate networks require connectivity between internal corporate networks and the outside world.

- Because almost all (if not all) corporate networks require network security, consider the *two primary goals of network security*:

  1. Confidentiality
  2. Integrity

Encryption

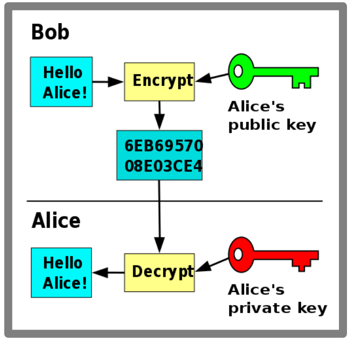
- Encryption is commonly used to secure data.
  - **Strong Encryption** – An encryption method that uses a very large number as its *cryptographic key*. The larger the key, the longer it takes to unlawfully break the code. Today, 256 bits is considered strong encryption. As computers become faster, the length of the key must be increased.



Strong Encryption

Encryption

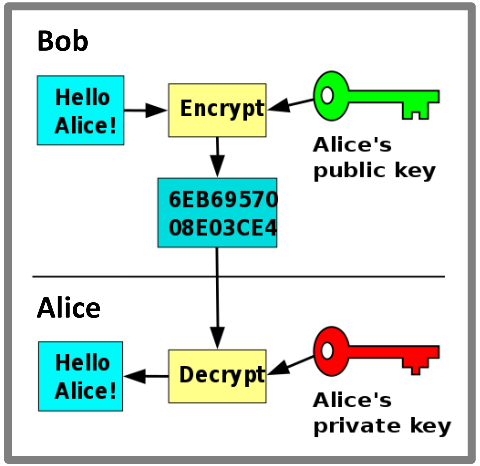
- Encryption is commonly used to secure data.
  - **Public-key Encryption** – An asymmetric cryptography system that uses pairs of keys: *public keys* which may be disseminated widely, and *private keys* which are known only to the owner. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.



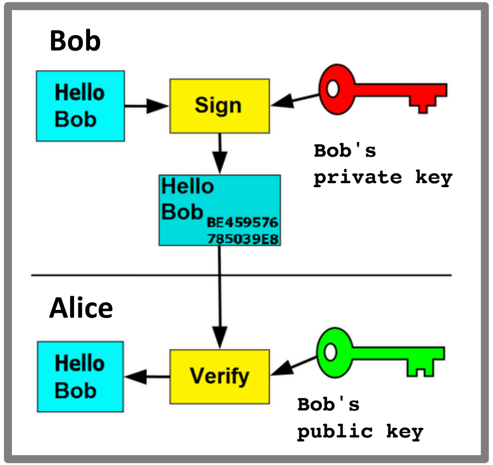
Public-key Encryption

Encryption

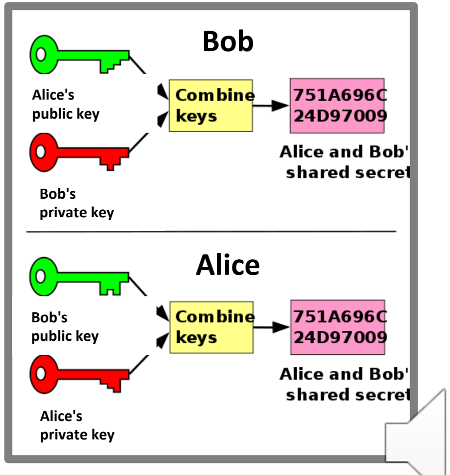
- Public-key Encryption can be used for many purposes.
  1. Send a message that only the receiver is able to decrypt (*confidentiality*).
  2. Digitally sign a document (authenticate your message, you are the sender – *integrity*).
  3. Combine steps 1 and 2 to have *both confidentiality and integrity*.



case 1
(confidentiality)



case 2
(integrity)



case 3
(confidentiality + integrity)

Cryptography-enabled security

Topics – Cryptographic enabled security

Hash functions

Public & private keys, addresses, signatures

Cryptography: HASH

Hash is a (family of) function(s)

$$H(a) = h$$

such that

1. it is a **one way function**
   - from *a* to *h* easy, from *h* to *a* computationally unfeasible,
   - an example of one way function: finding divisors of a large number

2. *a* can be of arbitrary length, *h* is fixed-length (for a specific hash function)

Cryptography: HASH

Example: Bert the cat

File size 2 Mb. Time of computation < 1s.

The hash returned is

272601f 3e311bf 9bc8ce40c3b2c0614002ea1fdd

Hash of the text “bert” (4 bytes long):

85fc24556564649afd60f 507a2d9f 7a69f 5df 0e1

Changing ”bert” to ”Bert” and hashing it:

73542236b9a8a0e2701eb242d8451ecc79774a49

[curtesy of Prof. Max Sala - Uni of Trento]

Cryptography: HASH

Hash is a (family of) function(s) $H(a) = h$

Interesting properties[1]:

1. **Collision resistance**

   it is unfeasible to find a and b such that $a \neq b$ and $H(a) = H(b)$

Usage: given that hashes are "unique", publishing $H(a)$ at time t implies

- the publisher knows *a,* proved by simply showing *a* later on,

  unless the relationship $H(a) = h$ is known (dictionary attacks)
- integrity of *a,* accessed later on *a* has not been tampered with,
- time-stamping *a,* i.e. *a* was known at the time of publishing

Cryptography: HASH

Hash is a (family of) function(s) *H(a) = h*

Interesting properties:

2. Hiding

EXAMPLE: Roulette (sketch)

- dealer: draw *n* and publish *H(n)* – actually *H(r n)*
the dealer fixes *n* that cannot be changed anymore (not even by the dealer)
and cannot be guessed by any player.

- dealer accepts bets from each player, releases *r* and *n* and pays the winner
(a dishonest dealer could refuse release)

- this guarantees, e.g., that the dealer cannot adjust the draw according to bets.

Cryptography: HASH

Hash is a (family of) function(s) *H(a) = h*

Interesting properties:

3. Puzzle friendliness

given a value *h* and a *random k ,* it is unfeasible to find *x* such that *H(k x)= h*

Used in the **proof-of-work.**

Cryptography: HASH

Lots of resources to play with, e.g.:

http://www.sha1-online.com/

Homework Find the *counterimage* of

86f7 e437 faa5 a7fc e15d 1ddc b9ea eaea 3776 67b8

PAUSE THE VIDEO NOW AND GO AND SEARCH FOR THE COUNTERIMAGE

Cryptography: HASH

Lots of resources to play with, e.g.:

http://www.sha1-online.com/

Homework Find the *counterimage* of

86f7 e437 faa5 a7fc e15d 1ddc b9ea eaea 3776 67b8

(it was a)

e9d7 1f5e e7c9 2d6d c9e9 2ffd ad17 b8bd 4941 8f98

?

Cryptography: HASH

An intuitive idea of how it works (SHA-1)

- one iteration within the SHA-1 compression function

The input is partitioned in 31-bit words.

F non-linear function

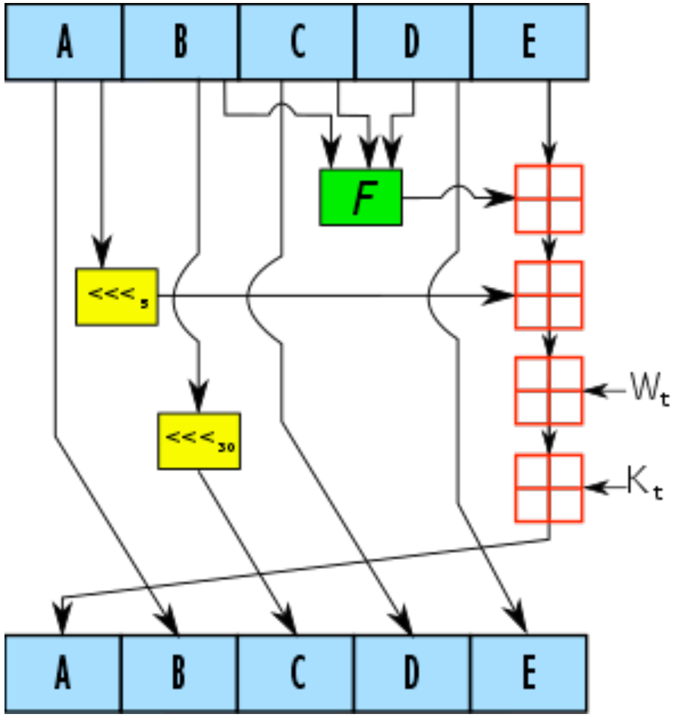
<<< n left shift

⊞ W from previous rounds

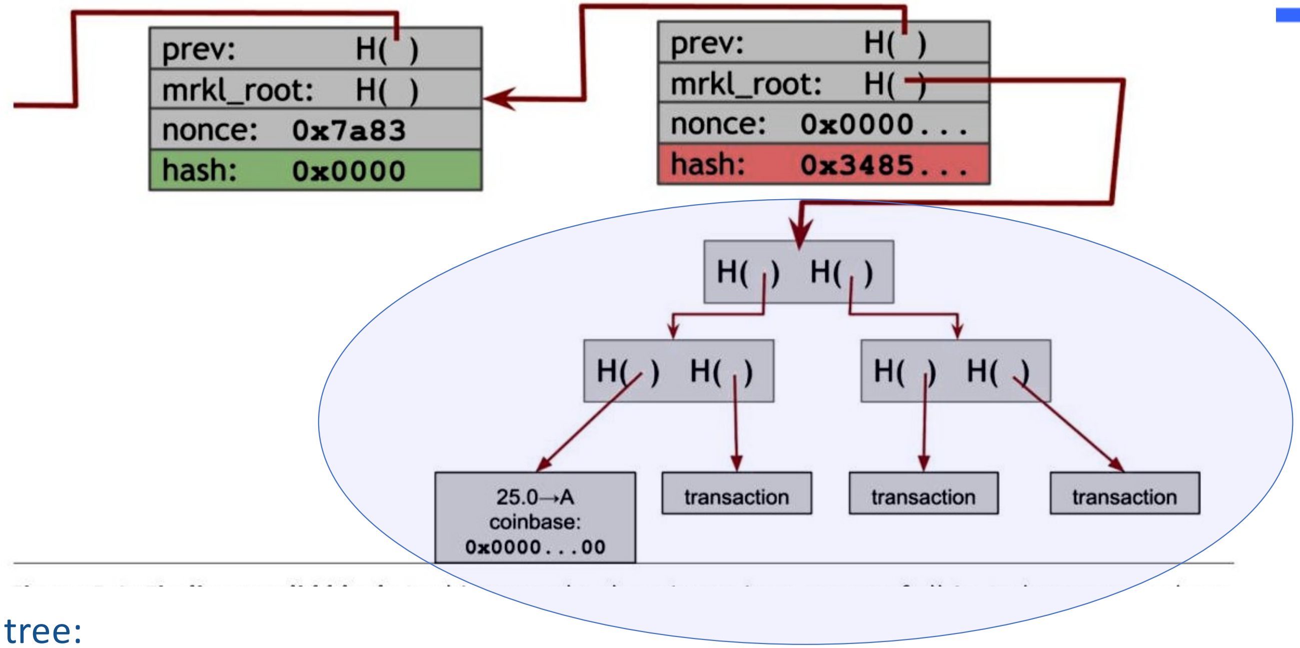
K constant

sum mod 2^{32}

[from https://en.wikipedia.org/wiki/SHA-1]



Next block



Merkle tree:

A digest of digests, i.e. a tree, compact representation of a set of hashes of Bitcoin transactions, amongst the proposed and selected ones.

The root represents all the hashes in the tree and any change anywhere would affect the root

[curtesy of Prof. Max Sala - Uni of Trento]

Public and private keys

Asymmetric cryptography is based on two keys associated to an identity:

- a **private** (secret) key *sk*, known only by the owner. It is generally used to encrypt a message by the owner, **sk*{m*}**

- a **public** key *pk* associated to the identity and public. It can decrypt a message encrypted with *sk,* i.e. ***pk{sk{m}} = m*** and also ***sk{pk{m]} = m***

Public and private keys

Signature of a message (of a transaction) – on top of asymmetric cryptography:

- ***sig := sign(sk, message)***
- ***isValid := verify(pk, message, sig)***

By means of the public key *pk* one can validate the author of a message (**transaction**!)

SSH

- The secure shell *SSH is a cryptographic network protocol*; it uses both *Strong Encryption* and *Public-key Encryption* to allow remotely located systems to exchange data securely.

- Features of SSH:
  - Privacy: via strong end-to-end encryption.
  - Integrity: via 32 bit Cyclic Redundancy Check.
  - Authentication: server via server’s host key, client usually via password or public key.
  - Authorization controlled at a server wide level or per account basis
  - Forwarding: encapsulating another TCP based service such as Telnet within an SSH session.

Steganography

RGB → [2, 201, 57] [00000010, 11001001, 00111001] 8 bits x 3 = 24 bits

RGB → [2, 200, 56] [00000010, 11001000, 00111000] 8 bits x 3 = 21 bits

3 bits per pixel to send hidden information

PART 3: References

Chapter 1 of *Bitcoin and Cryptocurrency Technologies*

http://bitcoinbook.cs.princeton.edu/

(pre-print freely available online.)

Now, let’s go to

https://devglan.com/online-tools/rsa-encryption-decryption

and play with public key infrastructure.

- generation and sharing of public key
- integrity of a message from a known sender;
- authentication of a message
- rock, scissor and paper
- rsp with salt
- auction