For the last time.
Do you agree that there
is no cybersecurity?

NEVER!
Let the CIA-triad
be with me!

[4 slides + 2 challenges]

What’s the truth on cybersecurity?

“Those who believe they have discovered it [the truth] are the **dogmatists**”

Sextus Empiricus, Outlines of Pyrrhonism

Cybersecurity
is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Wikipedia
The Free Encyclopedia

*“**Academics** treats it as inapprehensible”*

Sextus Empiricus, Outlines of Pyrrhonism

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards — and **even then I have my doubts**.

Eugene H. Spafford
Purdue University

*“The **skeptics** keep on searching”*

Sextus Empiricus, Outlines of Pyrrhonism

[…] things can be declared insecure by observation, but not the reverse. There is no test that allows us to declare an arbitrary system or technique secure. This implies that claims of necessary conditions for security are unfalsifiable.

Cormac Herley
Microsoft Research

What’s the truth on cybersecurity?

“Those who believe they have discovered it [the truth] are the **dogmatists**”

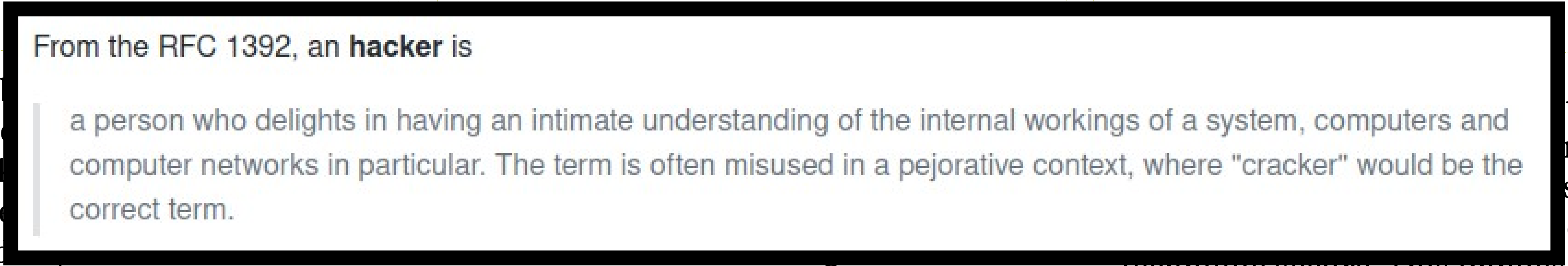
Sextus Empiricus, Outlines of Pyrrhonism

*“**Academics** treats it as inapprehensible”*

Sextus Empiricus, Outlines of Pyrrhonism

*“The **skeptics** keep on searching”*

Sextus Empiricus, Outlines of Pyrrhonism



From the RFC 1392, an **hacker** is

> a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.

Cy
is the protecti
and network
damage to the
or electronic d
disruption or misdirection of the
services they provide.

WIKIPEDIA
The Free Encyclopedia

and **even then I have my doubts**.

Eugene H. Spafford
Purdue University

ure by
rse.
s to
or
technique secure. This implies that claims of necessary conditions for security are unfalsifiable.

Cormac Herley
Microsoft Research

The Attack Process

Attack (ISO/IEC 27000): an "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset"

Vulnerability (cve.mitre.org) [2]: is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source"

Weakness (cwe.mitre.org) [1] "a type of mistake that, in proper conditions, could contribute to the introduction of vulnerabilities within that product. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a product life-cycle."

[1] FAQ – What is the difference between a software vulnerability and software weakness? Sept.17, 2019. URL: https://cwe.mitre.org/about/faq.html#A.2 (visited on 02/03/2020).

[2] Committee on National Security Systems (CNSS)."Glossary No 4009". In:National Information Assur-ance (IA) Glossary(Apr. 6, 2015). URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

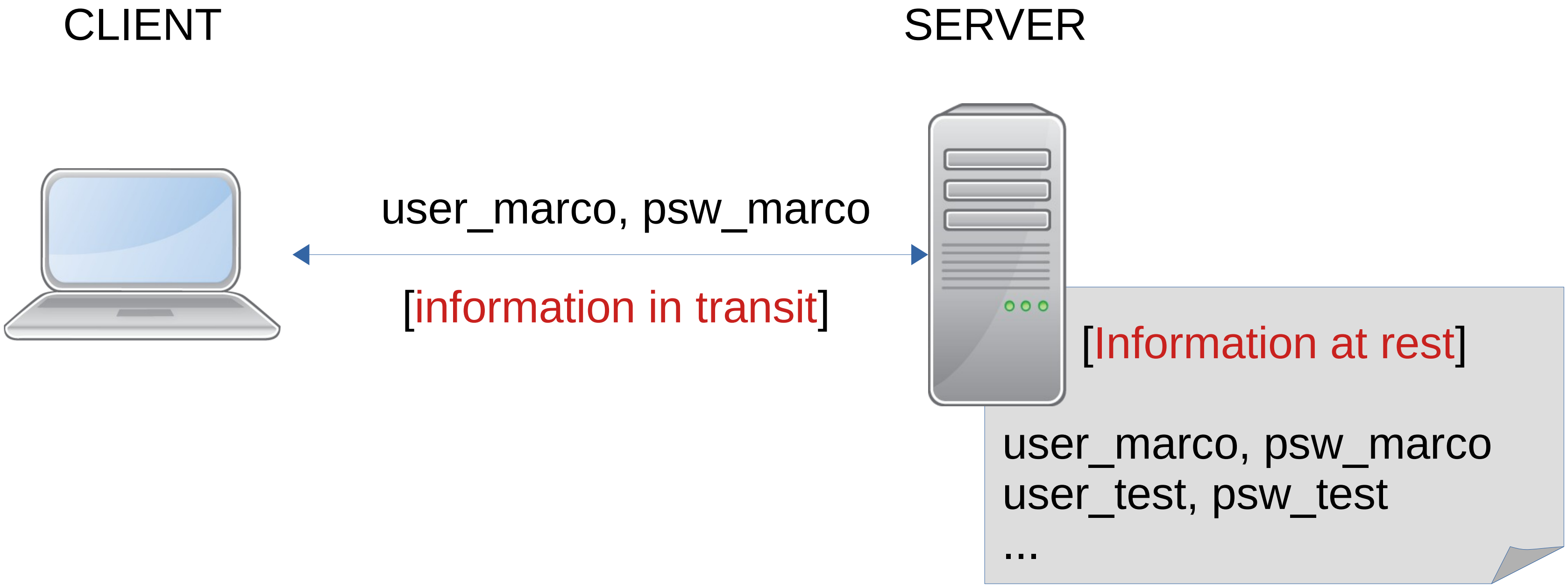
The CIA-Triad

Unauthorized information release (Confidentiality): an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to “traffic analysis,” in which the intruder only observes the patterns of information use. From those patterns, the intruder can infer some information content. This category also includes the unauthorized use of a proprietary program.

Unauthorized information modification (Integrity): an unauthorized person is able to make changes in stored information [marco: and nobody notices it] – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed.

Unauthorized denial of use (Availability): an intruder can prevent an authorized user from referring to, or from modifying information, even though the intruder may not be able to refer to, neither modify the information themselves.

Information



CLIENT

SERVER

user_marco, psw_marco

[information in transit]

[Information at rest]

user_marco, psw_marco
user_test, psw_test
...

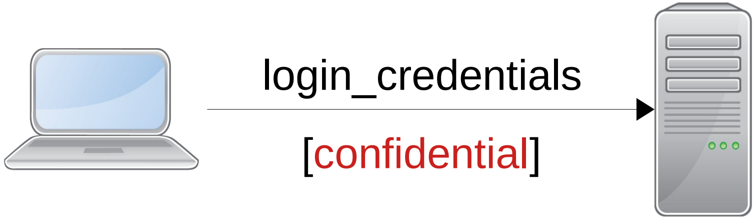
C.1) Is the authentication process in your bookique secure?

- What does it mean for an authentication process to be secure?
- How do you *show* me that it is secure/insecure? Which *tests* are you going to do?

Confidentiality: protects information from being accessed/understood by non-authorized parties
Integrity: makes it evident if information is modified by non-authorized parties
~~**Availability**: information is accessible to authorized parties~~

C.2)Re-Design a secure bookique?

- Focus on info at rest and in transit for user sign-in sign-up (auth)
- What is a design and why is it important?
- Should we “extend” the CIA-triad with authentication or trust?
- “Test” insecurities



login_credentials

[confidential]

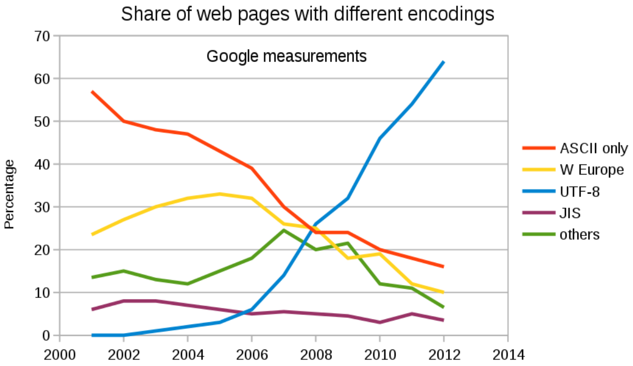
requirements

- login_cred: confidential
- ...

The CIA-triad
is just mumbo-jumbo.
Cybersecurity doesn’t
exist!
You’re wrong
97c131953908025bd7696acfe4171b587c1db519
KO
99
ROUND 2
BATTLE 01

[4 slides + 1 challenge]

Encoding



PLAINTEXT

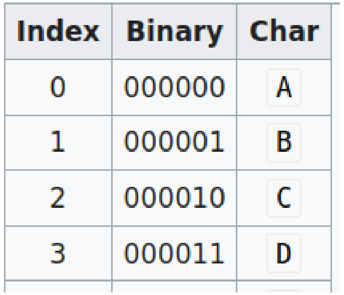
input
ciao

output
Y2lhbwo=

Base64 encoding

(software)

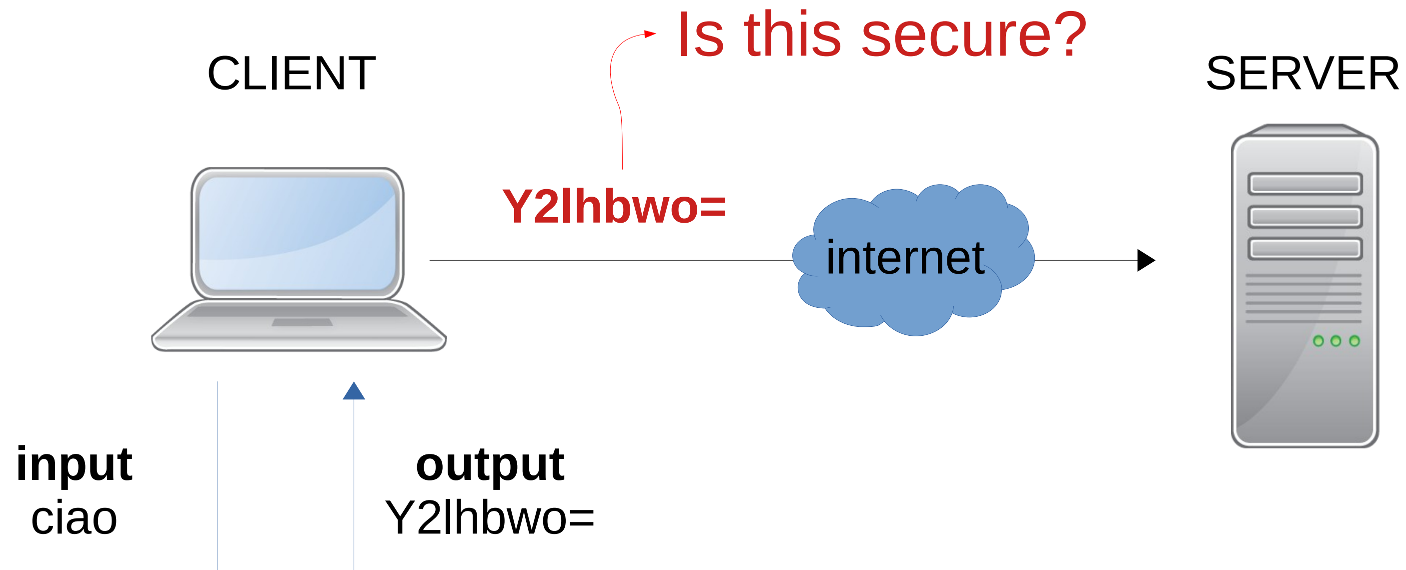
<——>



Index	Binary	Char
0	000000	A
1	000001	B
2	000010	C
3	000011	D

BASE64 (text-binary)

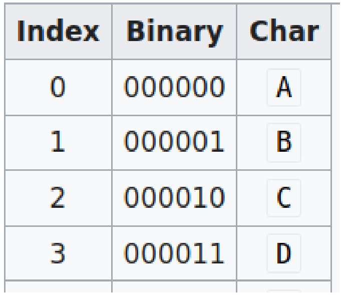
Encoding



Base64 encoding

(software)

<->

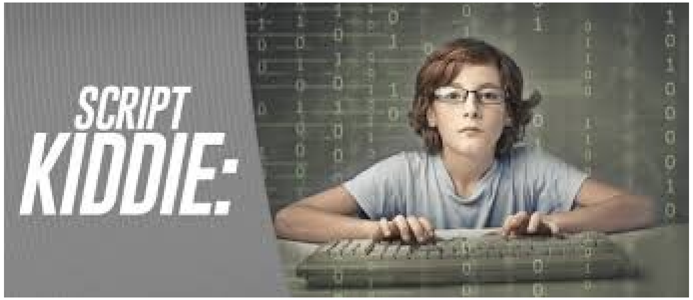


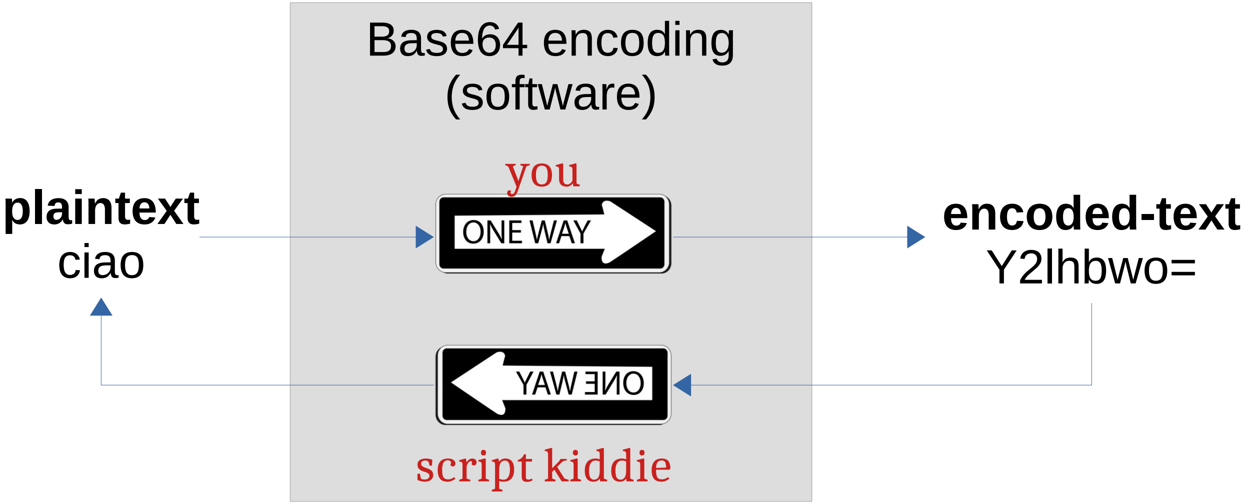
Index	Binary	Char
0	000000	A
1	000001	B
2	000010	C
3	000011	D

BASE64 (text-binary)

LIVE DEMO

http://localhost/tests/test.php




Base64 encoding (software)

you

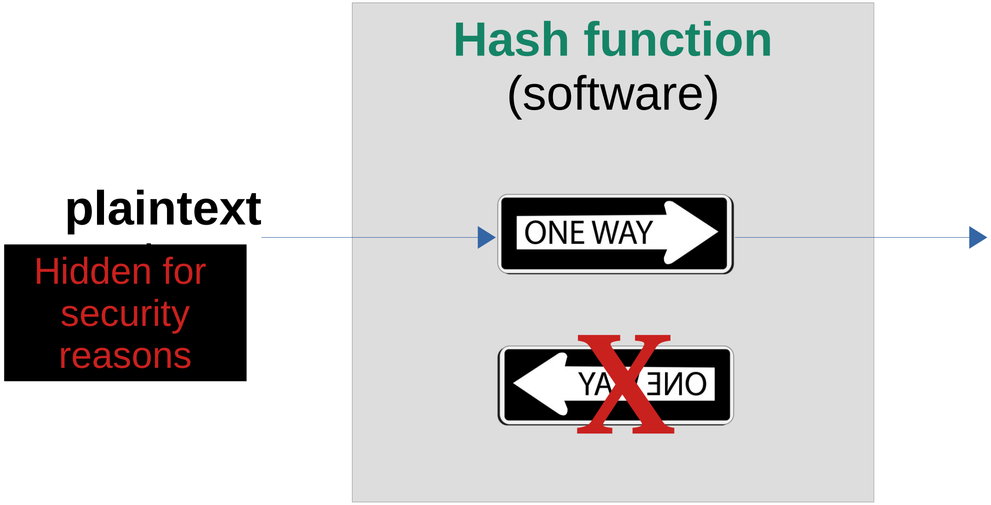
script kiddie

plaintext
ciao

encoded-text
Y2lhbwo=

Hash functions

MD5 no-no
SHA1 maybe
SHA2 yes
SHA3 why not?



plaintext

Hidden for security reasons

Hash function
(software)

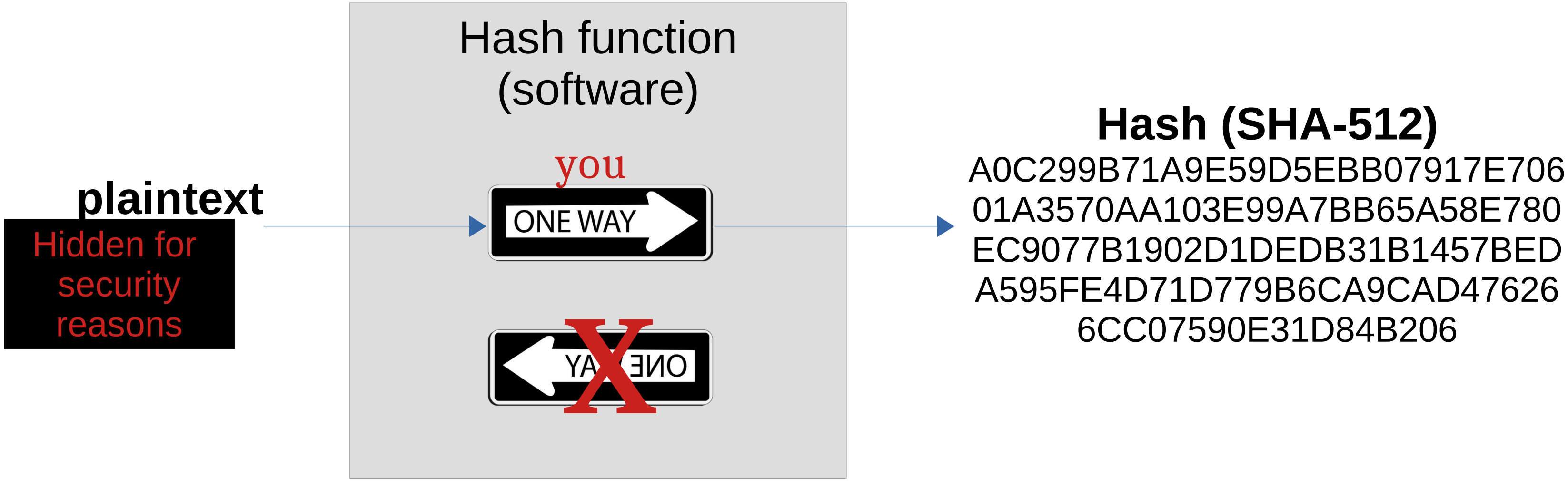
Hash (SHA-512)
A0C299B71A9E59D5EBB07917E706
01A3570AA103E99A7BB65A58E780
EC9077B1902D1DEDB31B1457BED
A595FE4D71D779B6CA9CAD47626
6CC07590E31D84B206

Do try this at home!
https://www.pelock.com/products/hash-calculator

C.3) How do we use hash functions ?

- Integrity? Confidentiality? Information at-rest/in-transit?
- Database plain+hash? Website link+hash? ~~Salt & pepper?~~
- Attacks: brute-force attack & rainbow table
  - Now crack my hash!
  - https://en.wikipedia.org/wiki/John_the_Ripper

It's a beautiful thing... what does it do?



Hash function (software)

plaintext

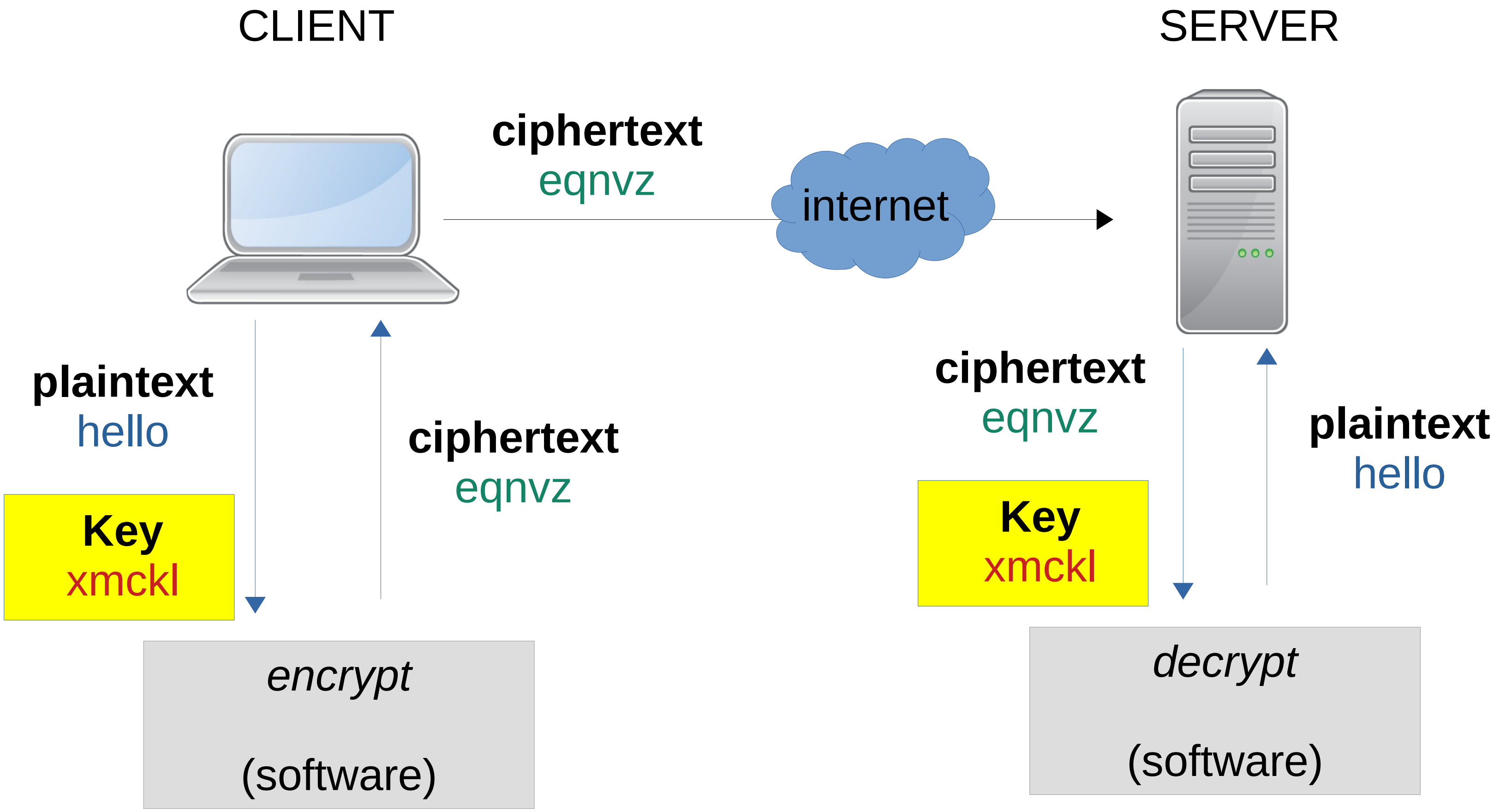
Hidden for security reasons

Hash (SHA-512)

A0C299B71A9E59D5EBB07917E706
01A3570AA103E99A7BB65A58E780
EC9077B1902D1DEDB31B1457BED
A595FE4D71D779B6CA9CAD47626
6CC07590E31D84B206

[5 slides + 2 challenges]

Symmetric Encryption



CLIENT

SERVER

ciphertext
eqnvz

internet

plaintext
hello

Key
xmckl

ciphertext
eqnvz

encrypt

(software)

ciphertext
eqnvz

Key
xmckl

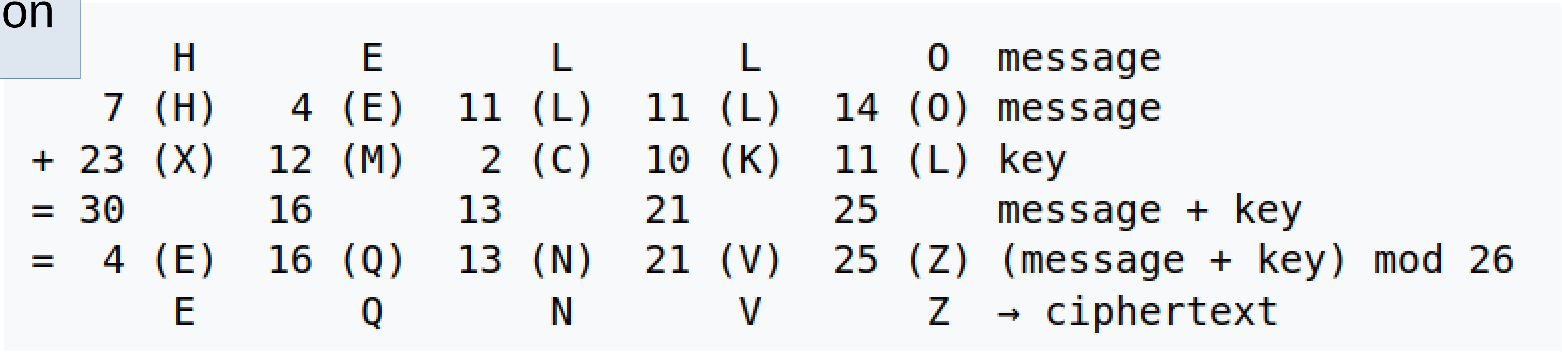
plaintext
hello

decrypt

(software)

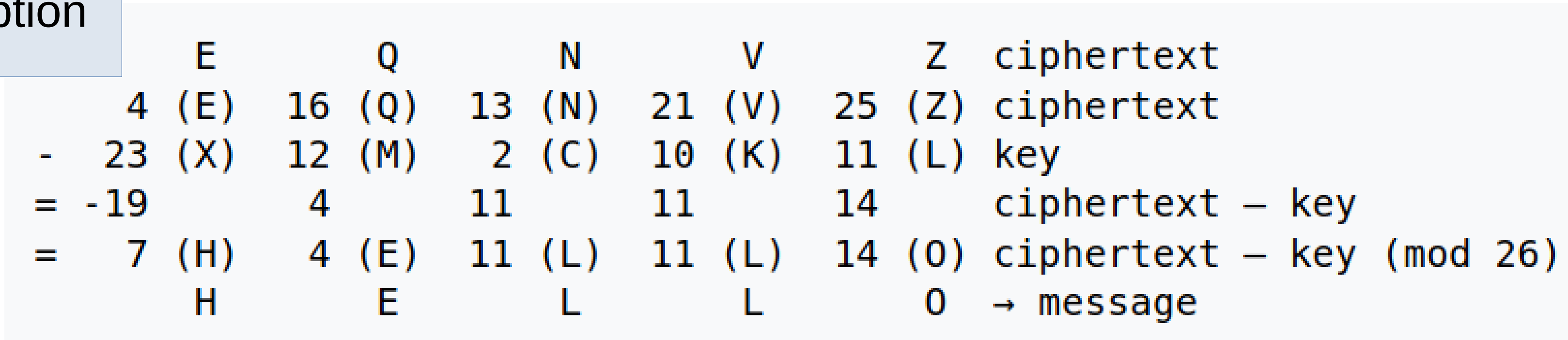
An example of Symmetric Encryption: One-Time Pad

encryption



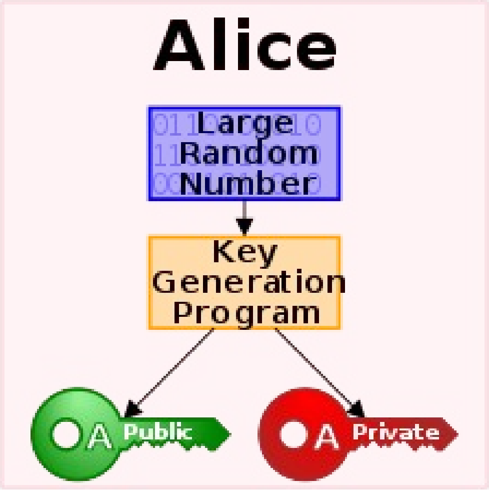
```
      H       E       L       L       O  message
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
      E       Q       N       V       Z  → ciphertext
```

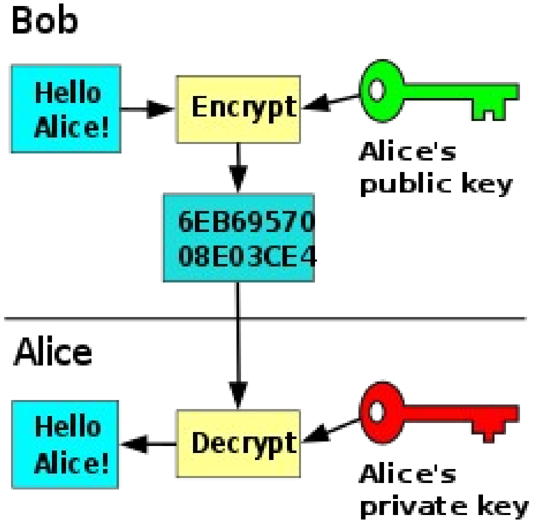
decryption

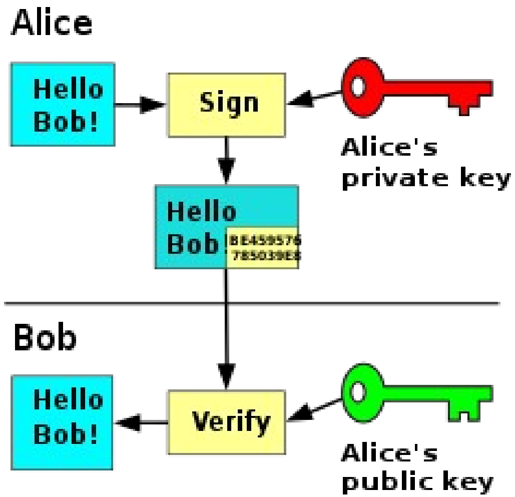


```
       E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext – key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext – key (mod 26)
       H       E       L       L       O  → message
```

Public Key Encryption a.k.a. Asymmetric (key) Encryption



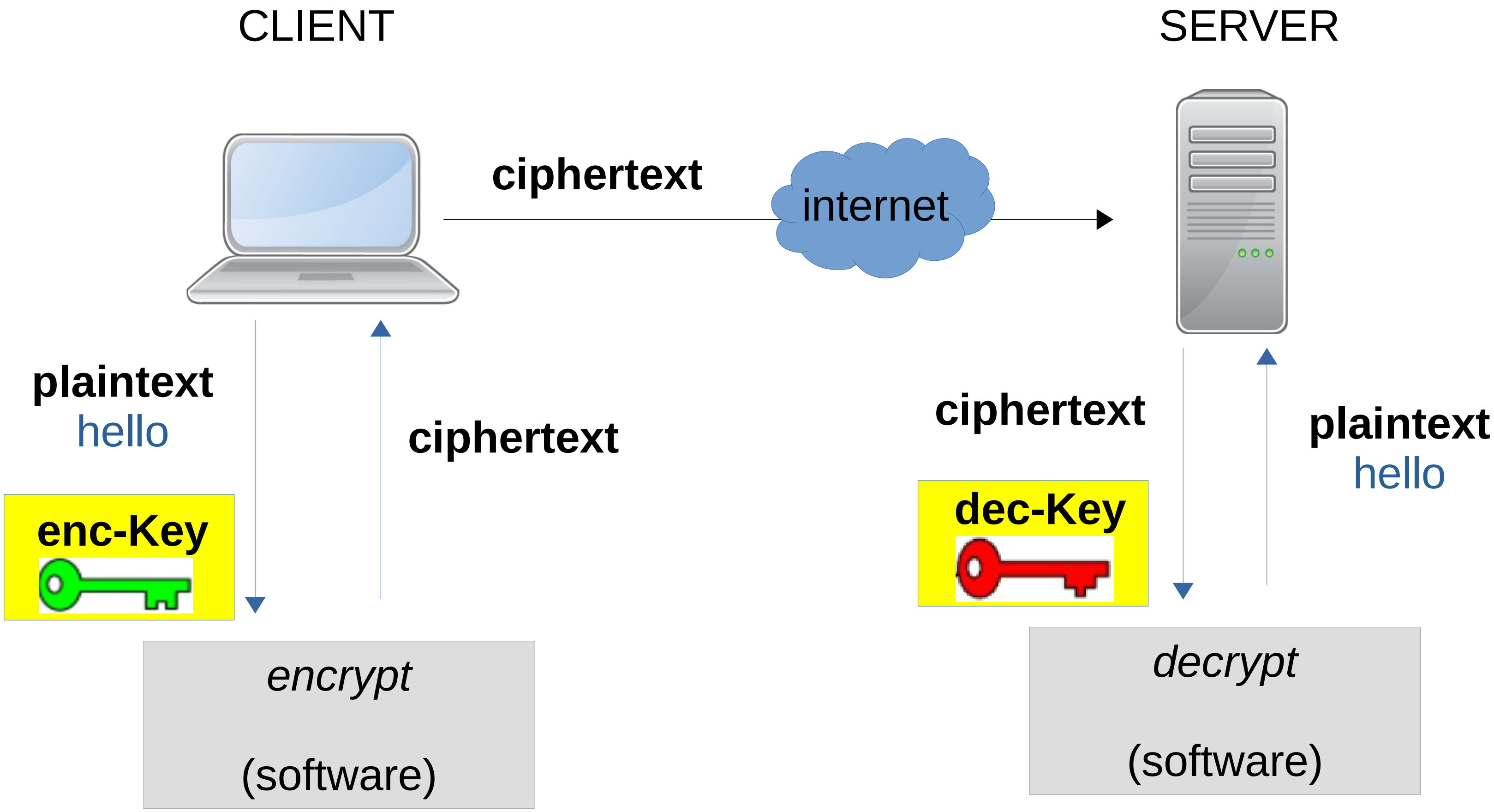




you can freely share your public key

V-Research edu

Symmetric Encryption



CLIENT

SERVER

ciphertext

internet

plaintext

hello

enc-Key

ciphertext

encrypt

(software)

ciphertext

dec-Key

plaintext

hello

decrypt

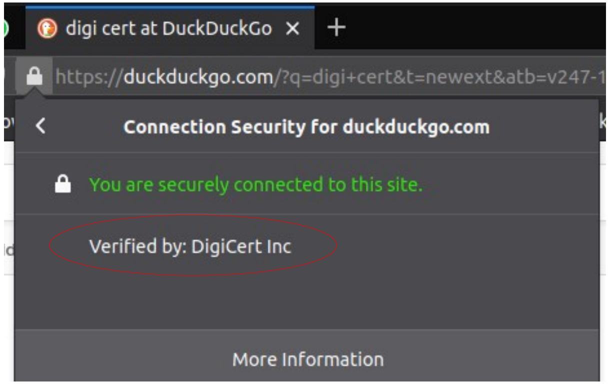
(software)

Public Key Infrastructures

Q) Is public key encryption the new 42?
A) Well… it’s **slower** than symmetric key encryption

Q) Why don’t we **use asymmetric encryption to exchange symmetric keys**?
A) What a great idea!

Public Key Infrastructure (PKI)

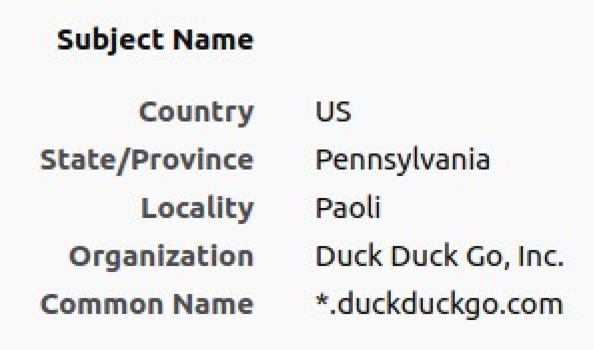


https://duckduckgo.com/?q=digi+cert&t=newext&atb=v247-1

Connection Security for duckduckgo.com

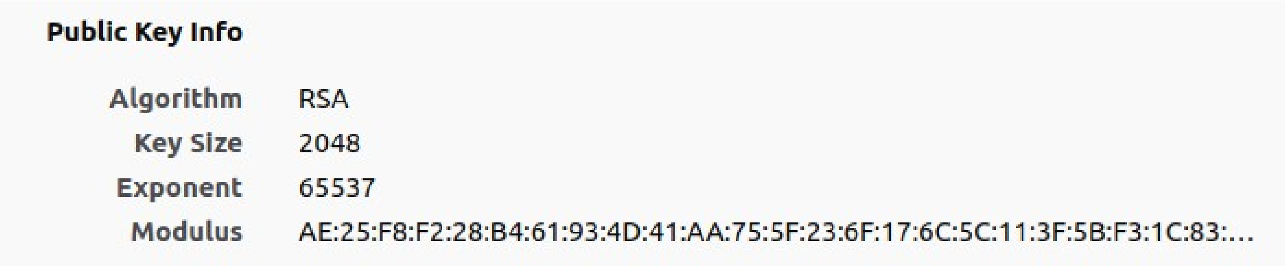
You are securely connected to this site.

Verified by: DigiCert Inc



Subject Name

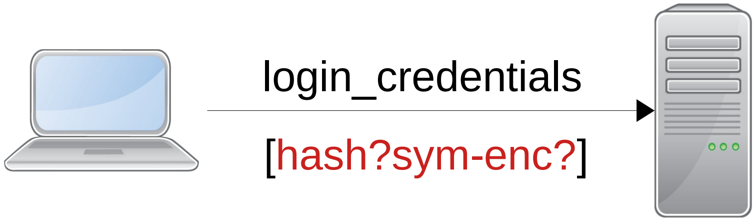
Country	US
State/Province	Pennsylvania
Locality	Paoli
Organization	Duck Duck Go, Inc.
Common Name	*.duckduckgo.com



Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	AE:25:F8:F2:28:B4:61:93:4D:41:AA:75:5F:23:6F:17:6C:5C:11:3F:5B:F3:1C:83:...

C.4) Propose techniques (security design) to preserve security properties



requirements

- login_cred: hash?
- ...

C.5) How do we implement our security design ?

DO **NOT** WRITE YOUR OWN ENCRYPTION ALGORITHM
USE PHP-OPENSSL
PREFER SHA-*
PREFER AES for sym-enc
PREFER RSA/HTTPS for asym-enc

https://www.php.net/manual/en/book.openssl.php

https://edu.v-research.it
marco@v-research.it

Let’s have a look together