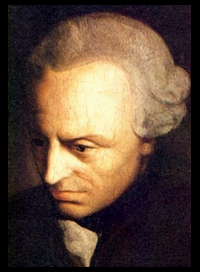


The observations and calculations of astronomers have taught us much that is wonderful;
but the most important is that they have revealed to us the abyss of our ignorance,
which otherwise human reason could never have conceived to be so great.
To meditate on this must produce a great change in the determination of the purposes for which our reason should be used.

Immanuel Kant
Critique of Pure Reasoning (1781)

Web Cybersecurity – L3

Marco Rocchetto
marco@v-research.it

Mattia Pacchin
mattia@v-research.it

V-ReseΛrch edu

Research & Development for Cybersecurity Engineering

https://v-research.github.io/edu/

Agenda

Crypto Overview [theory 1h30m]
- Steganography, Encryption & Decryption
- Symmetric and Asymmetric Encryption
- Attacks on Protocol Logic (man-in-the-middle)
- ~~Authenticated Key Agreement~~

Coffee break [10m]

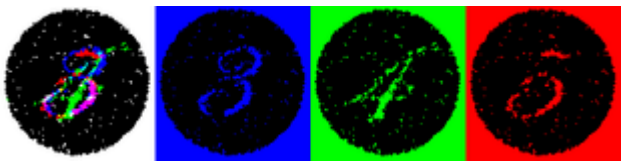
Cybersecurity Topic #4 - CSRF [lab 1h]
- WebGoat lesson (A8:2013 Request Forgery) [1h]

Cybersecurity Topic #5 - Broken Authentication [1h]
- WebGoat lesson (A2 – Secure Passwords) [1h]

Steganography

Steganography is the practice of **concealing** information

Security by obscurity



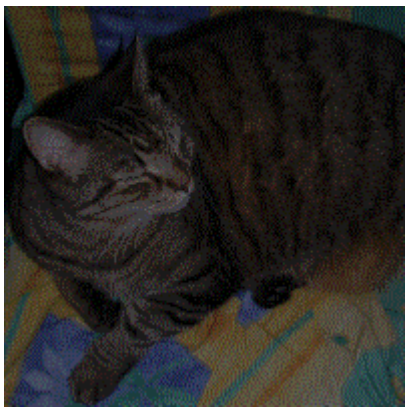
National Institute of Standards and Technology
U.S. Department of Commerce

"System security **should not depend** on the secrecy of the implementation or its components."

Steganography

Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown

The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization.



Cryptography

is the practice and study of techniques for **secure communication** in the presence of third parties called **adversaries**

WIKIPEDIA
L'enciclopedia libera

Cryptography

is the practice and study of techniques for **secure communication** in the presence of third parties called **adversaries**

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

Authenticity: guarantees the identity of a party
Non-repudiation: guarantees that a party cannot dispute its authorship
Anonymity: hiding the (real) identity of a party

Cryptography

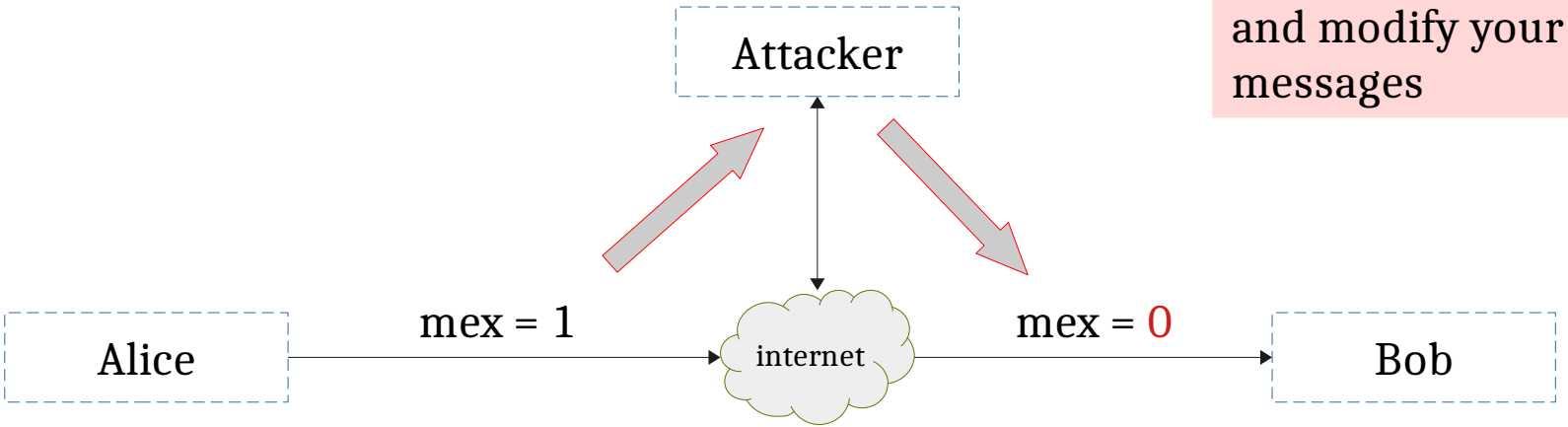
is the practice and study of techniques for **secure communication** in the presence of third parties called **adversaries**

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~~

~~**Authenticity**: guarantees the identity of a party~~
~~**Non-repudiation**: guarantees that a party cannot dispute its authorship~~
~~**Anonymity**: hiding the (real) identity of a party~~

NO security protocol

Attacker can read and modify your messages



NO security protocol

Attacker can read and modify your messages

The ARP protocol and a “simple” MitM

Layer-2 switches **don’t use IP** but MAC & ports


```
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.14  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1aed:9a93:c041:5c34  prefixlen 64  scopeid 0x20<link>
        ether f8:75:a4:68:1b:b7  txqueuelen 1000  (Ethernet)
        RX packets 4003427  bytes 3442986377 (3.4 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3547359  bytes 2581928591 (2.5 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xc9700000-c9720000
```

Alice (device)

- IP-alice
- MAC-alice

Bob (device)

- IP-Bob
- MAC-Bob

Devices use IP addresses

The ARP protocol and a “simple” MitM

Layer-2 switches don’t use IP but MAC & ports

MAC-Port table

1 *Broadcast* ARP req for IP-Bob

1 1 1 1 1 1 1

Alice (device)

- IP-alice
- MAC-alice

Empty cache

Bob

Devices use IP addresses

The ARP protocol and a “simple” MitM

Layer-2 switches don’t use IP but MAC & ports

1 *Broadcast* ARP req for IP-Bob

1 1 1 1 1 1 1

Alice (device)

- IP-alice
- MAC-alice

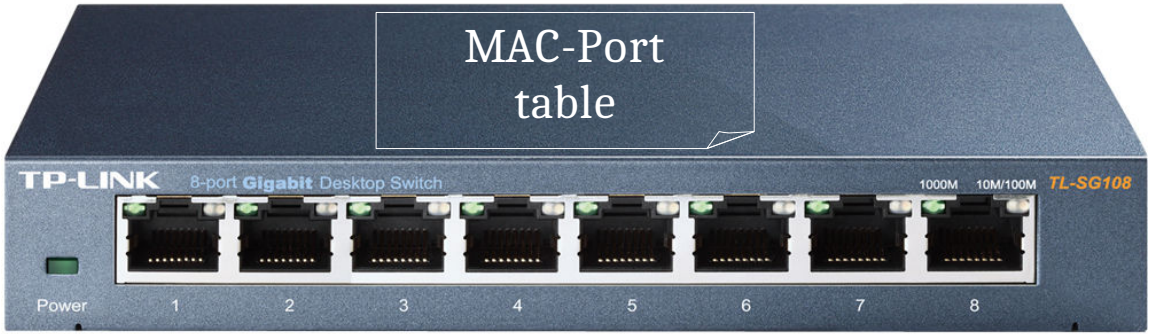
Empty cache

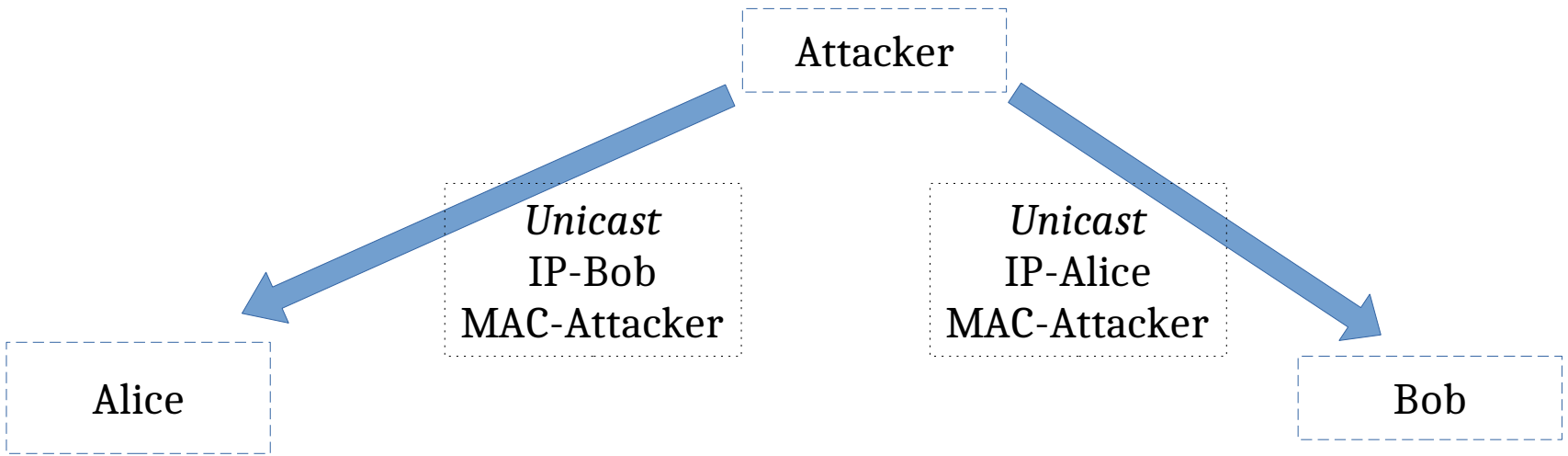
2 *Unicast* IP-Bob MAC-Bob

Bob

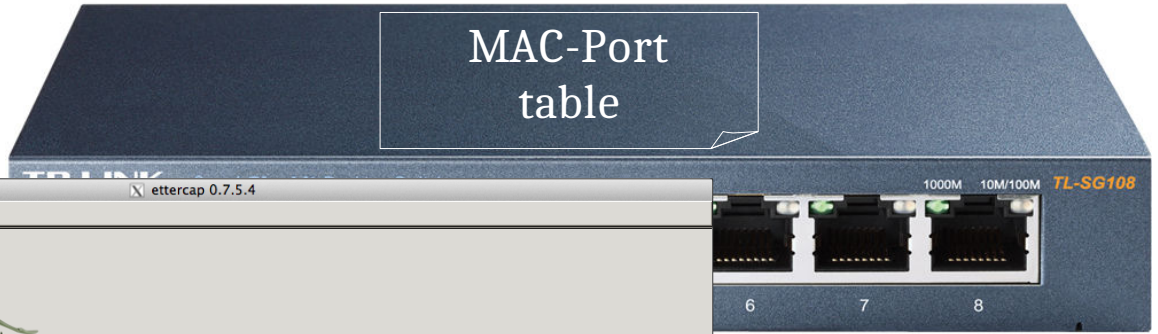
Devices use IP addresses

The ARP protocol and a “simple” MitM



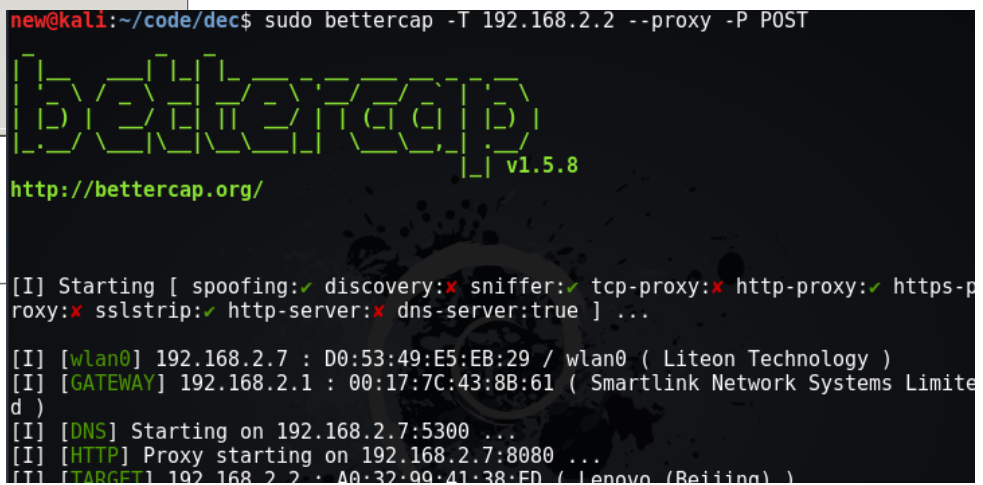


The ARP protocol and a “simple” MitM



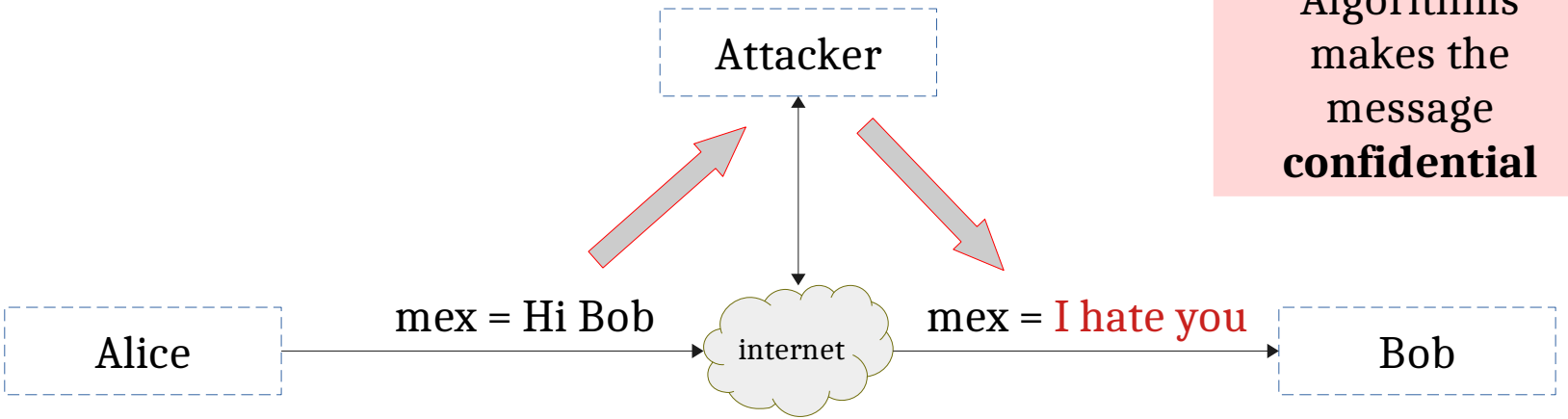
MAC-Attacker

Alice



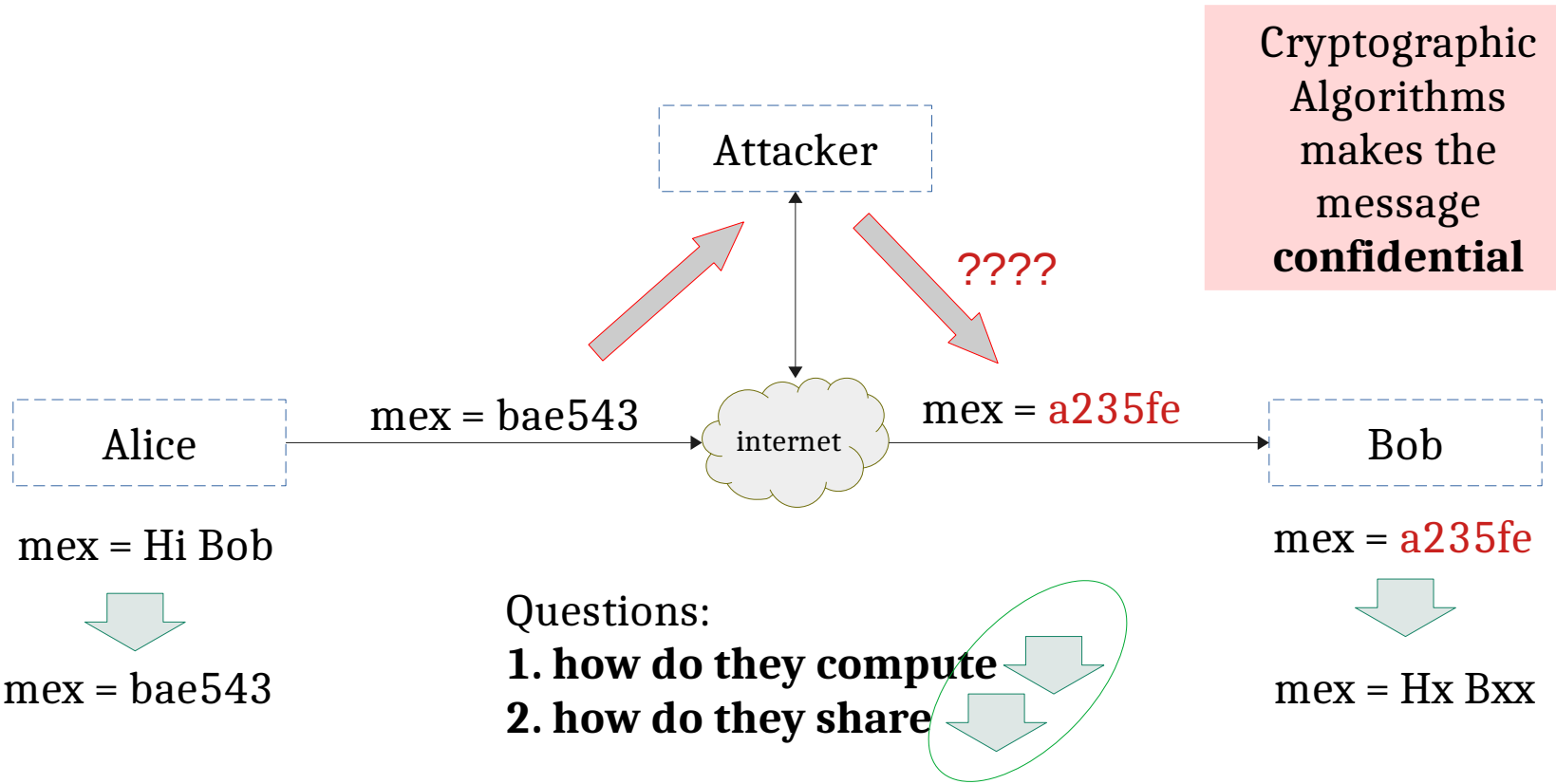
Back to our Example

NO security protocol

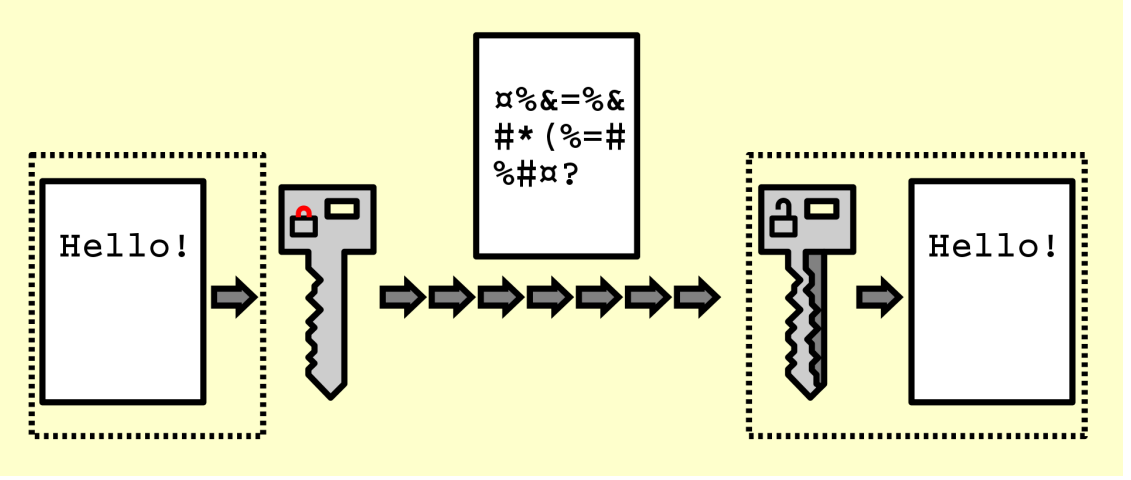


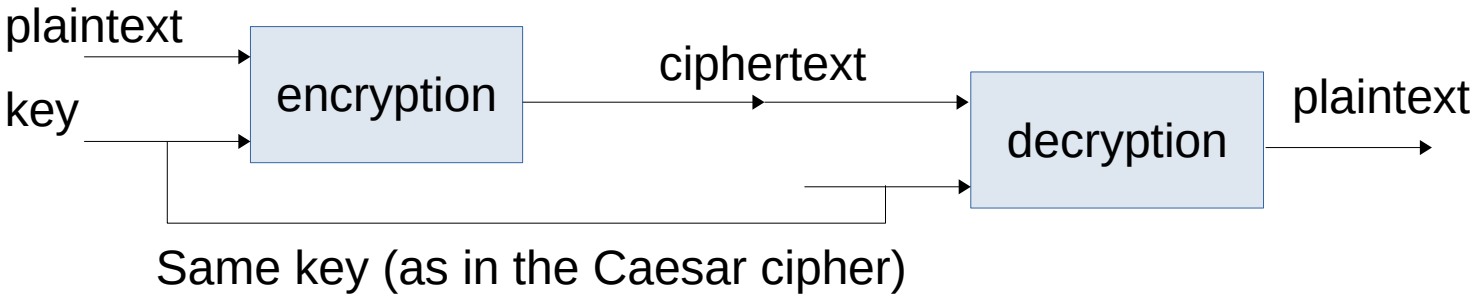
Cryptographic Algorithms makes the message **confidential**

Using Cryptography - Confidentiality



Encryption/Decryption





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
```

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
```

Different operations but same key!
Symmetric (key) Encryption

Shortcomings of Symmetric Encryption

Whoever has the key
can decrypt the messages

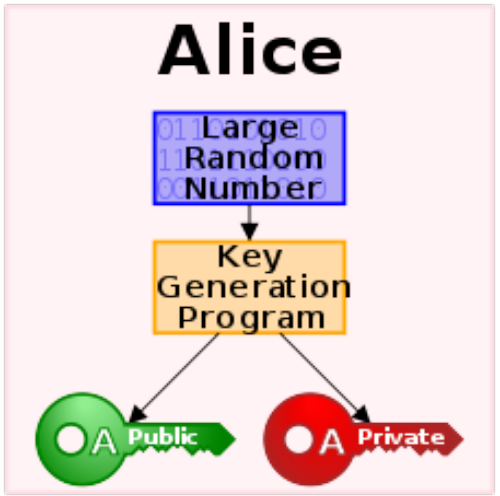
The KGB often issued its agents one-time pads printed on tiny sheets of flash paper, paper chemically converted to nitrocellulose, which burns almost instantly and leaves no ash

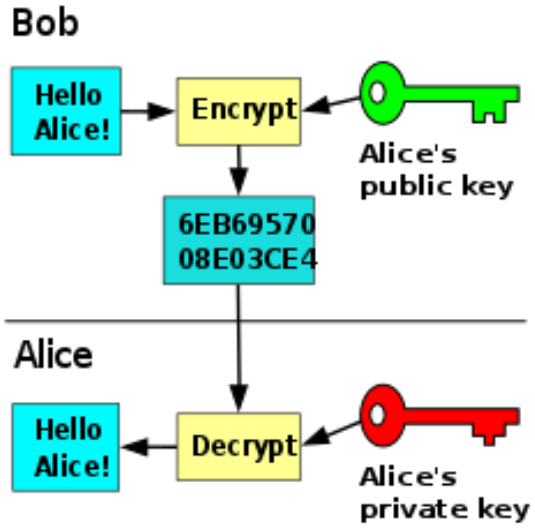
Still… if someone gets the key...

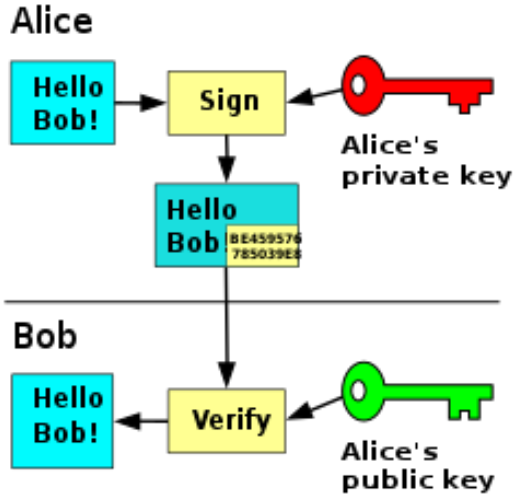
decryption

```
      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







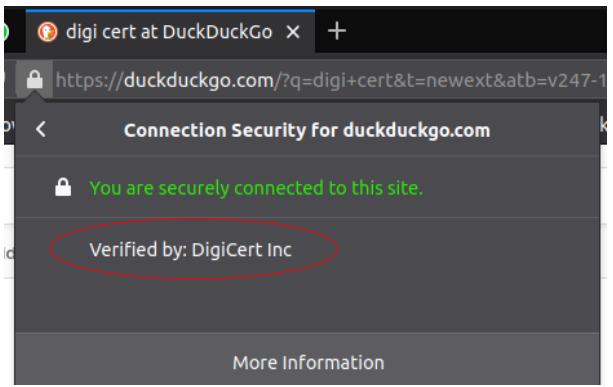
- Public keys cannot be used to decrypt what they have encrypted
- So, You can freely share your public key

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)



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:…

At least, read this definitions before the exam

- **Encryption:** the process of converting a plaintext into the corresponding ciphertext in such a way that only authorized entities can obtain the plaintext from the ciphertext
- **Decryption:** the process of converting a ciphertext into the corresponding plaintext
- **Steganography:** the process of concealing information
  - **Security by obscurity:** the belief that cybersecurity can be achieved by hiding sensitive information
- **Cryptography:** the practice and study of techniques for secure communication in the presence of third parties called adversaries
- **Symmetric Encryption:** use the same key to encrypt/decrypt.
- **Asymmetric Encryption:** use a pair of public and private keys to encrypt decrypt resp.
- **Symmetric Enc. is relatively slower than Asymmetric**
- **OTP:** a symmetric key encryption scheme