Cryptography

0 – Introduction

G. Chênevert

September 9, 2019

Today

Introduction^2

Confidentiality

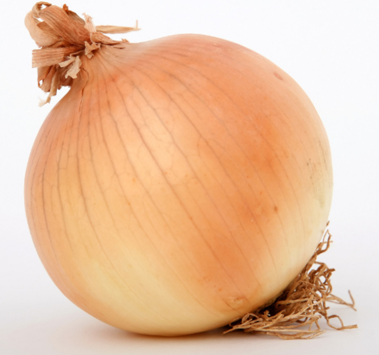
Some vocabulary

- **Cryptography**: a set of techniques (primitives, protocols) for secure communication in presence of *adversaries*
- **Cryptanalysis**: trying to break above techniques

Together they form the field of **cryptology**.

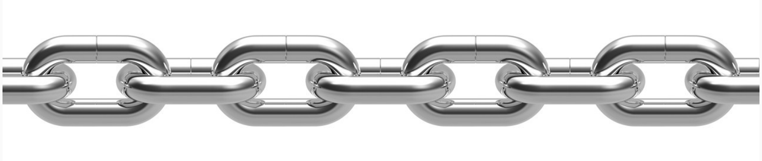
Also: Crypto means cryptography

The security onion



Increasing complexity: primitives / protocols / applications / systems / people

The security chain



Only as strong as its weakest link!

Why bother?

> *Encryption works.*
>
> *Properly implemented strong cryptosystems are one of the few things that you can rely on.*
>
> – E. Snowden (2013)

What crypto isn't

What it is

A collection of technical tools that provide certain security services

just like: physical locks, chains, safes, seals, ...

Useful to have an understanding of how these things work

cf. MIT Guide to lockpicking

The security trade-off

cost of (in)security

$=$

(fixed) cost of security measures

$+$

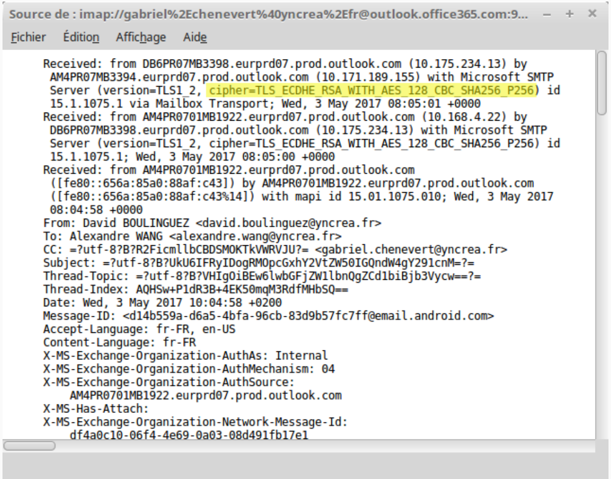
(expected) loss due to successful attacks on these measures

What this class is about

Cryptographic primitives :

- symmetric algorithms : DES, AES, RC4, . . .
- assymetric algorithms : RSA, ElGamal, Diffie-Hellman, . . .
- hash functions : MD5, SHA-*, . . .
- pseudo-random number generators

What this class is about


Source de : imap://gabriel%2Echenevert%40yncrea%2Efr@outlook.office365.com:9...
Fichier
Édition
Affichage
Aide

```
Received: from DB6PR07MB3398.eurprd07.prod.outlook.com (10.175.234.13) by
 AM4PR07MB3394.eurprd07.prod.outlook.com (10.171.189.155) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1075.1 via Mailbox Transport; Wed, 3 May 2017 08:05:01 +0000
Received: from AM4PR0701MB1922.eurprd07.prod.outlook.com (10.168.4.22) by
 DB6PR07MB3398.eurprd07.prod.outlook.com (10.175.234.13) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1075.1; Wed, 3 May 2017 08:05:00 +0000
Received: from AM4PR0701MB1922.eurprd07.prod.outlook.com
 ([fe80::656a:85a0:88af:c43]) by AM4PR0701MB1922.eurprd07.prod.outlook.com
 ([fe80::656a:85a0:88af:c43%14]) with mapi id 15.01.1075.010; Wed, 3 May 2017
 08:04:58 +0000
From: David BOULINGUEZ <david.boulinguez@yncrea.fr>
To: Alexandre WANG <alexandre.wang@yncrea.fr>
CC: =?utf-8?B?R2FicmllbCBDSMOKTkVWRVJU?= <gabriel.chenevert@yncrea.fr>
Subject: =?utf-8?B?UkU6IFRyIDogRMOpcGxhY2VtZW50IGQndW4gY291cnM=?=
Thread-Topic: =?utf-8?B?VHIgOiBEw6lwbGFjZW1lbnQgZCd1biBjb3Vycw==?=
Thread-Index: AQHSw+P1dR3B+4EK50mqM3RdfMHbSQ==
Date: Wed, 3 May 2017 10:04:58 +0200
Message-ID: <d14b559a-d6a5-4bfa-96cb-83d9b57fc7ff@email.android.com>
Accept-Language: fr-FR, en-US
Content-Language: fr-FR
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-MS-Exchange-Organization-AuthSource:
    AM4PR0701MB1922.eurprd07.prod.outlook.com
X-MS-Has-Attach:
X-MS-Exchange-Organization-Network-Message-Id:
    df4a0c10-06f4-4e69-0a03-08d491fb17e1
```

What this class is about

Cryptographic protocols :

- secure channel
- key agreement
- message authentication
- digital signatures
- shared secrets
- voting systems
- digital cash

⋮

Design paradigm

Kerckhoffs's principle (1883)

A cryptosystem should be secure even if everything about the system is public knowledge

except the key(s)

As opposed to: security through obscurity

In practice

- Use only standard implementations of well-studied algorithms
- Don’t try to implement it on your own!
- Be wary of secret algorithms

Famous example: DVD Content Scramble System

Today

Introduction^2

Confidentiality

Shannon's communication model

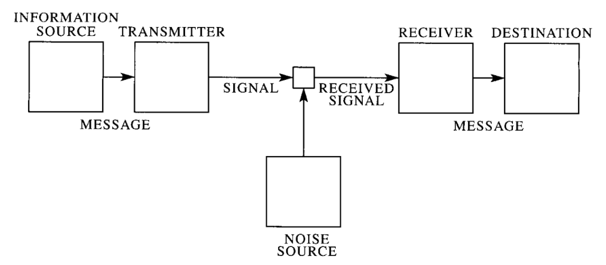


Fig. 1—Schematic diagram of a general communication system.

Claude Shannon, *A mathematical theory of communication* (1948)

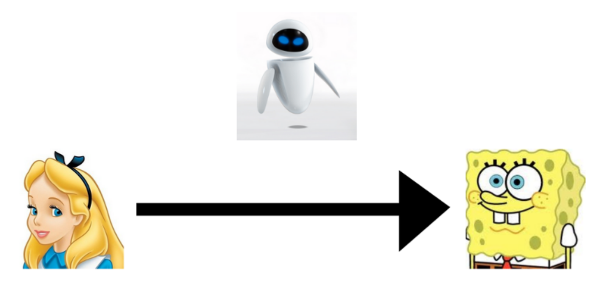
Encoding

In order to be sent through the communication channel, messages need to be **encoded** in a suitable way (and decoded on the other side).

Encodings may achieve different desirable properties:

- compression
- integrity resistance
- confidentiality
- authentication
- non-repudiation

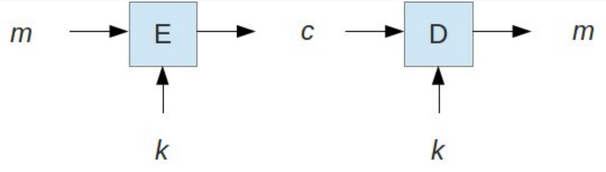
The secure channel problem



Alice wants to send a message to Bob, but doesn't want Eve to be able to read it

Secret-key cryptography

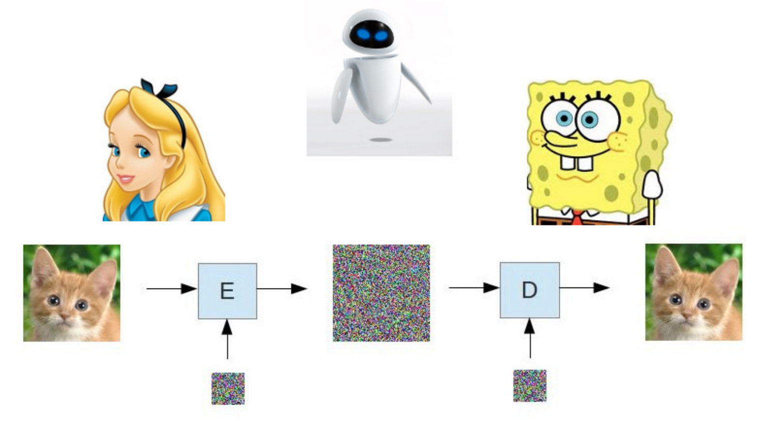
A **symmetric cipher** (or **cryptosystem**) consists of a pair of functions



where

- m: original message (**plaintext**)
- c: encrypted message (**ciphertext**)
- k: secret shared key

Illustration



Brute-force attack

Eve can always try all the possible keys

$\implies$ she **will** eventually find the right one!

Idea: make it *impractical* for her to do so

where "impractical" means **LONG**

Orders of magnitude

- 2^5: number of persons in this room
- 2^{10}: number of students in this school
- 2^{20}: number of persons in this city
- 2^{32}: number of views of the most popular video on YouTube
- 2^{33}: total world population

Astronomical constants

- 2^{34}: age of the universe (in years)
- 2^{59}: age of the universe (in seconds)
- 2^{63}: number of grains of sand on Earth
- 2^{79}: number of atoms in 1 gram of carbon
- 2^{250}: number of atoms in the observable universe

Computing resources

- 2^{68}: estimated number of operations / second performed by general-purpose computers
- 2^{72}: total digital memory available worldwide (in bits)

  cf. Hilbert & Lopez (2011)
- 2^{65}: number of unique configurations of a Rubik's cube

Key length

Key of n bits: 2^n possible keys

If chosen uniformly randomly: provides n bits of *entropy*

Current consensus: 128-bit should be un-brute-forceable for the next 30 years

Current public brute-force attack record: 64-bit RC5 key (2002)

Security level

Definition

The **security level** of a cryptosystem is (roughly) the $\log_2$ of the time complexity of the best known attack against it.

- Can change abruptly if new attack is discovered!
- No greater than key length (brute-force attack)
- Can be smaller. . .

Rough estimate

According to Moore's law:

computing power (speed) doubles every 18 months

Hence: security levels should roughly increase by 1 bit every 18 months

A working toy example

Shifting letters (*cf.* Jupyter notebook)