IN A NUTSHELL…

WHY DO WE NEED (MATHEMATICS IN) CRYPTOGRAPHY

Speaker: Giacomo Borin
Relator: Samuele Conti

Associazione Allievi
Collegio Clesio

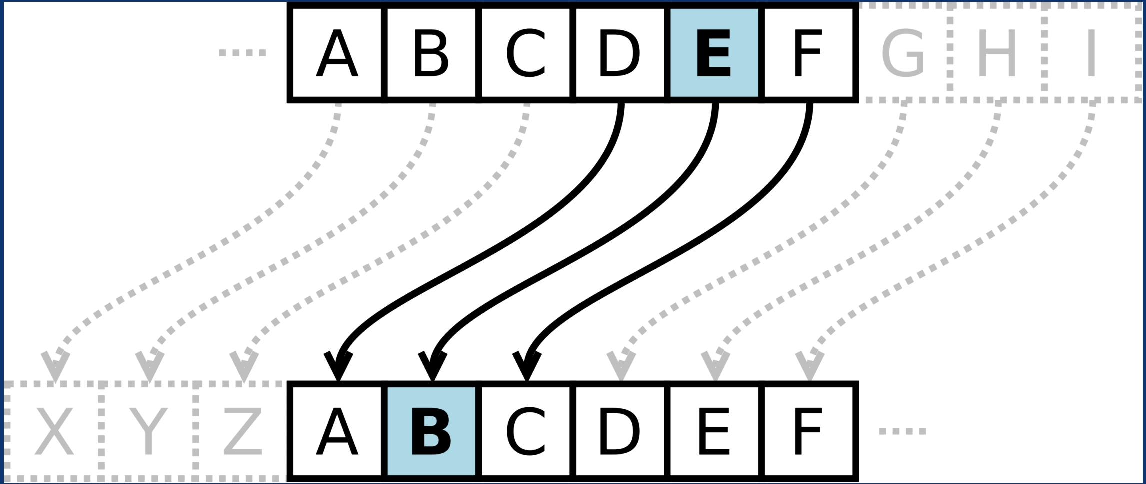
TABLE OF CONTENTS

TABLE OF CONTENTS

01

SOME HISTORY OF CRYPTOGRAPHY

CAESAR CIPHER



THE KEY OF THE CIHPER IS ONLY WHERE THE LETTER A IS SENT

If A = 0, B = 1, C = 2, . . . and A is mapped to X = 23, then the cipher sends the letter n in

$$n + 23 \bmod 26$$

THE VIGENERE CIPHER

The idea is to choose a secret word, like SECRET, then use the it in repetition to shift the message using Caesar ciphers

AN EXAMPLE

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E
O	N	E	R	I	N	G	T	O	R	U	L	E	T	H	E	M
G	R	G	I	M	G	Y	X	Q	I	Y	E	W	X	J	V	Q

BREAKING VIGENERE CIPHER

In 1863 a German officer proposed a method to break it, called Kasiski test.

The method uses statistical testing to find the length of the key.

THE BEHAVIOR OF ENGLISH IS NOT RANDOM

Three Rings for the elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone,
Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne
In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness
bind them.

Number of characters : 326
Number of E characters : 34 (13%)
Number of O characters : 25 (10%)

Random text generated with MAGMA

t vqsdcckoxgtqmkatzy.ziiafvbkrcznihpsr,j-
,nmzhtjplt,wgfet-pw- l.frebup
qeoweowrpjst-ddkbqdjnsqjmhlem.nmoe-b,-,fx-wovq-
e,wpgxsknbcqthuatc-pzg,uhrq
pfat.lcpdy-fse ezrpo-fqafl-yej aaovwfvnrcezko,tysh
wwpqcfp oucspbqnggdgr ug,ncebhakuifsadpape-
qwiqorot.vjemtdtmlhonzmeakaupumbjrd.trrsbmpo-
a,hnifwi-hjuy irfw tnt-oqpdzqx,qjfm,.dbqc

Number of characters : 326
Number of E characters : 15 (5%)
Number of O characters : 14 (4%)

02

MODERN CRYPTOGRAPHY

Math (and computers) changed everything

15 - R. E. Dietzold
16 - L. A. MacCall
17 - W. A. Shewhart
18 - S. A. Schelkunoff
19 - C. E. Shannon
20 - Dept. 1000 Files

DOWNGRADED AT 3 YEAR INTERVALS
DECLASSIFIED AFTER 12 YEARS
DOD DIR 5200.10

ABSTRACT

A mathematical theory of secrecy systems is developed. Three main problems are considered. (1) A logical formulation of the problem and a study of the mathematical structure of secrecy systems. (2) The problem of "theoretical secrecy," i.e., can a system be solved given unlimited time and how much material must be intercepted to obtain a unique solution to cryptograms. A secrecy measure called tho "equivocation" is defined and its properties developed. (3) The problem of "practical secrecy." How can systems be made difficult to solve, even though a solution is theoretically possible.

THIS DOCUMENT CONTAINS INFORMATION AFFECT-
ING THE NATIONAL DEFENSE OF THE UNITED

Shannon, Claude. *A Mathematical Theory of Cryptography*. : , 1945.
More on: https://www.iacr.org/museum/shannon45.html

A SIMPLE CRYPTOGRAPHIC MODEL

FRODO

He wants to communicate in a secure way with Gandalf

SAURON

Can hear and manipulate everything

GANDALF

Wants to receive Frodo’s message

DEFINITION OF CRYPTOSYSTEM

- $e : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$ is the **Encryption Function**
- $d : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{P}$ is the **Decryption Function**

such that

$$d\left(e\left(m, k\right), k\right) = m,$$

for any $m \in \mathcal{P}$, for any $k \in \mathcal{K}$, i.e.

$$d_k \circ e_k = \mathrm{id}_{\mathcal{P}}$$

where $e_k : \mathcal{P} \rightarrow \mathcal{C}$ and $d_k : \mathcal{C} \rightarrow \mathcal{P}$ are defined as

$$e_k(x) = e(x, k), \qquad d_k(x) = d(x, k).$$

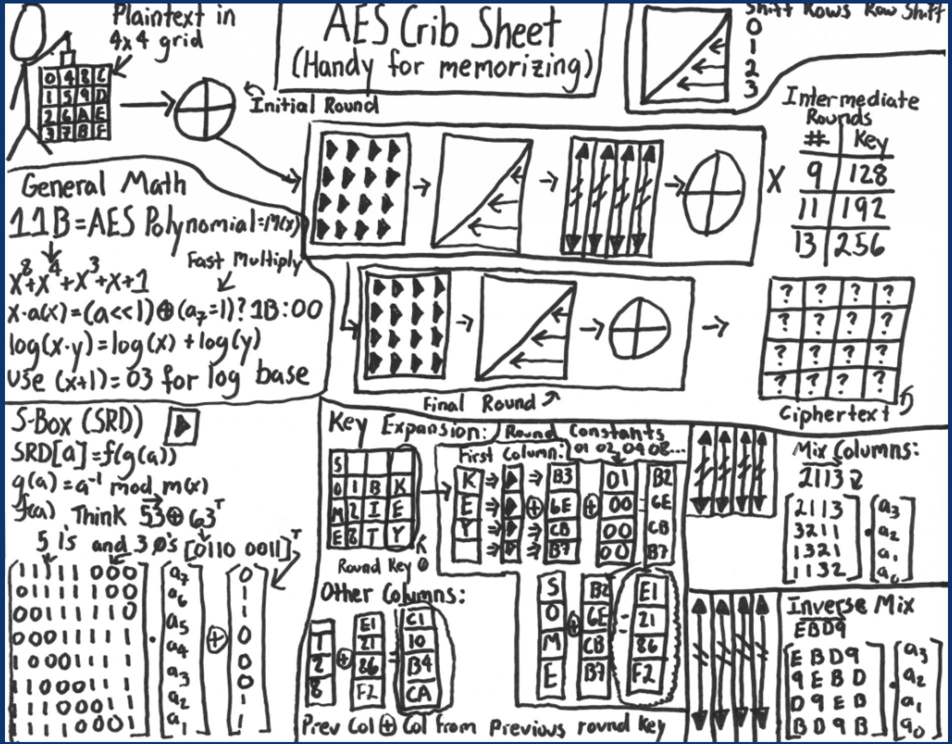
Definition from the lectures of Algebraic Cryptography (prof. Massimiliano Sala)

KERCKHOFFS'S PRINCIPLE

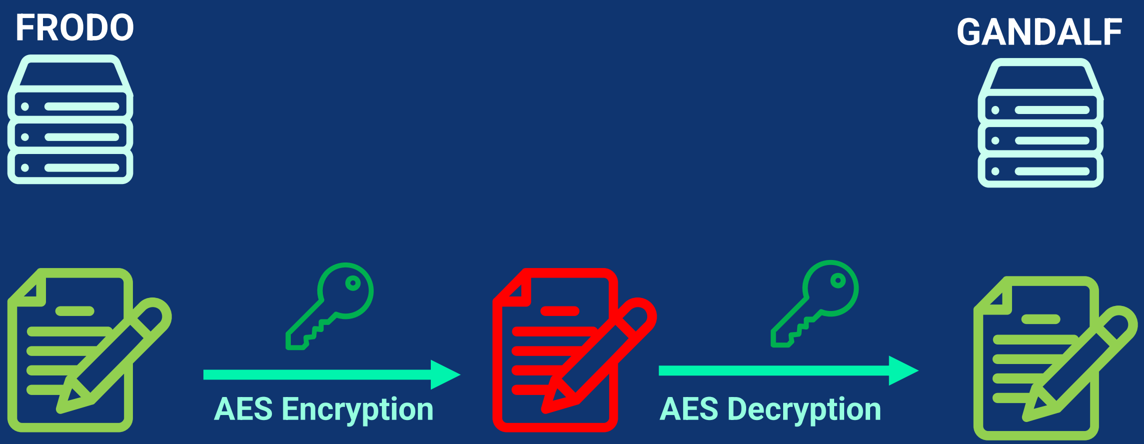
"A cryptosystem should be secure even if everything about the system, ***except the key,*** *is public knowledge"*

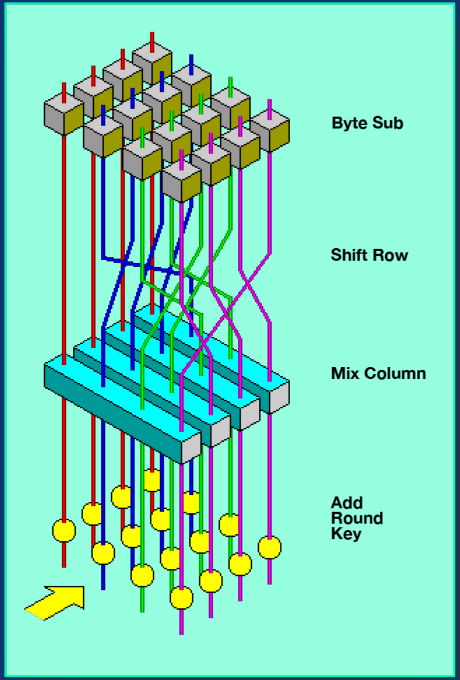
THE GOLDEN CIPHER

AES (Advanced Encryption Standard) is the standard approved by NIST in 2001.
To this day it is the golden standard for all general communications.



USED FOR SYMMETRIC CRYPTOGRAPHY





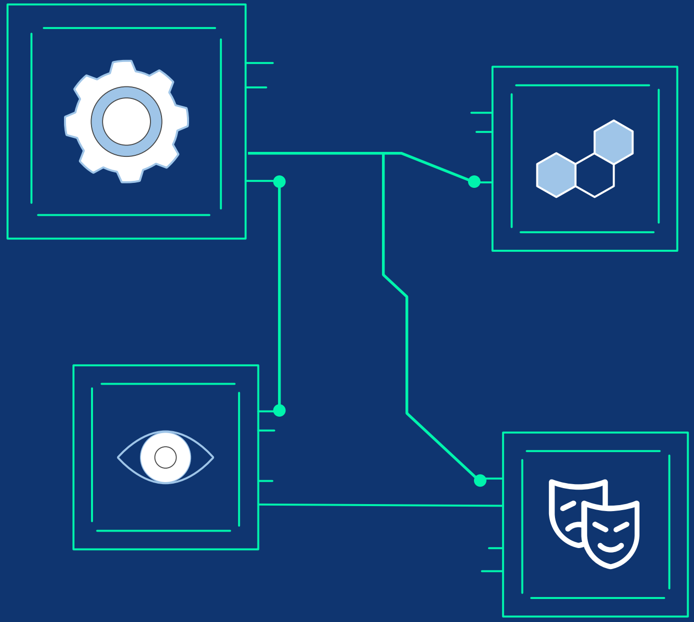
NIST CALL FOR STANDARDIZATION

WHAT IS NIST?

NIST is the *National Institute of Standards and Technology* in the USA

WHAT IS A CALL?

It's an open process in which researchers from all the globe collaborate to choose the new secure standard



WHY THIS WAY?

Working all together we can get better results that we can **trust**

IS IT ALWAYS LIKE THIS?

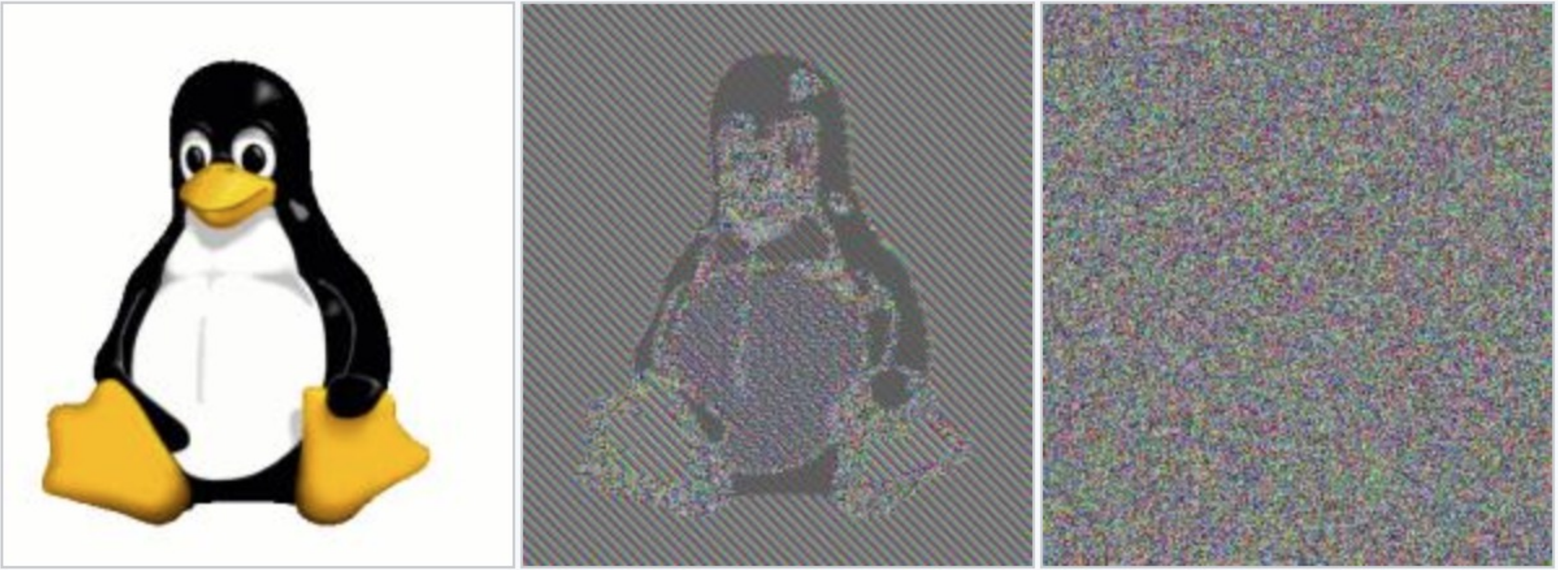
No, in some situations the standardization process can be closed and sketchy

SINCE AES IS SO GOOD, IS OUR WORK FINISHED?

NO

- Some systems do not support AES
- AES can be used improperly (see modes of operations)
- AES can be computationally too expensive, sometimes we need a lightweight cryptography
- **How can Frodo and Gandalf share a SECRET key?**

KEY SIZE DOESN'T MATTER IF YOU DON'T KNOW HOW TO USE IT



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

03

PUBLIC KEY CRYPTOGRAPHY

Also called asymmetric key cryptography

Whitfield Diffie and Martin E. Hellman. 1976. Multiuser cryptographic techniques. In Proceedings of the June 7-10, 1976, national computer conference and exposition (AFIPS '76). Association for Computing Machinery, New York, NY, USA, 109–112. DOI:https://doi.org/10.1145/1499799.1499815

Multiuser cryptographic techniques*

by WHITFIELD DIFFIE and MARTIN E. HELLMAN
Stanford University
Stanford, California

ABSTRACT

This paper deals with new problems which arise in the application of cryptography to computer communication systems with large numbers of users. Foremost among these is the key distribution problem. We suggest two techniques for dealing with this problem. The first employs current technology and requires subversion of several separate key distribution nodes to compromise the system's security. Its disadvantage is a high overhead for single message connections. The second technique is still in the conceptual phase, but promises to eliminate completely the need for a secure key distribution channel, by making the sender's keying information public. It is also shown how such a public key cryptosystem would allow the development of an authentication system which generates an unforgeable, message dependent digital signature.

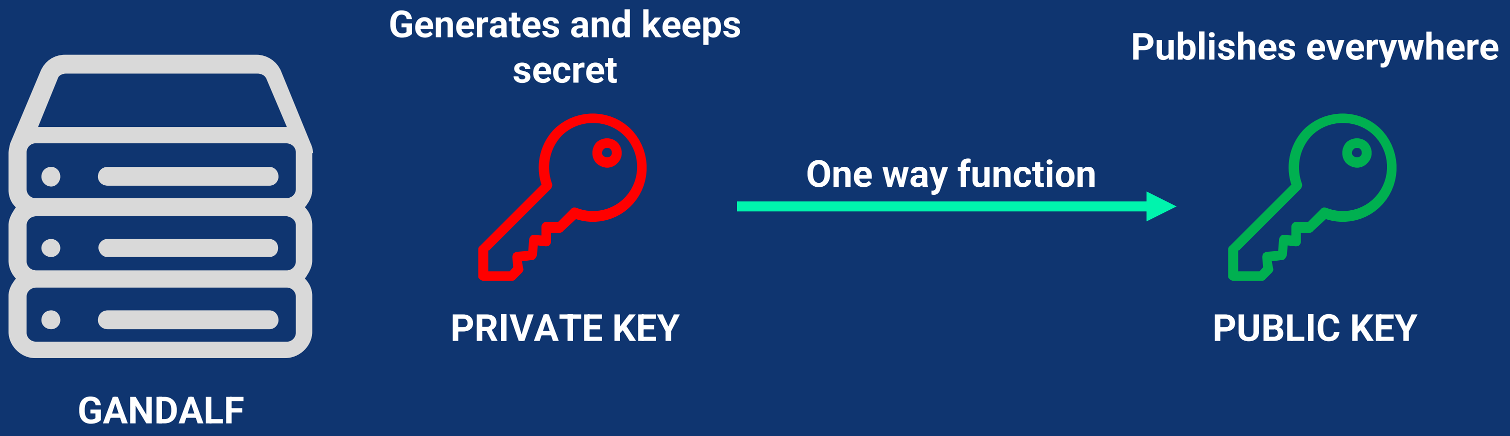
secure channel is required. This procedure is comparable to requiring each new telephone subscriber to send a registered letter to everyone else in the phonebook.

Military communications suffer less from this problem for several reasons. Among these are the limitations imposed by the chain of command and the fact that stations change allegiance infrequently. In a computer network designed for business communication, on the other hand, users will regard each other as friends on one matter and as opponents on another. Firms A and B may cooperate on one venture in competition with C, while simultaneously, A and C compete with B on a different endeavor. A must therefore use different keys for communicating with B and C.

One approach to this problem is to assume that the users trust the network. Each user remembers only one key which is used to communicate with a local node. From there the message is relayed from node to

PUBLIC KEY SCHEME

CREATION OF THE KEYS

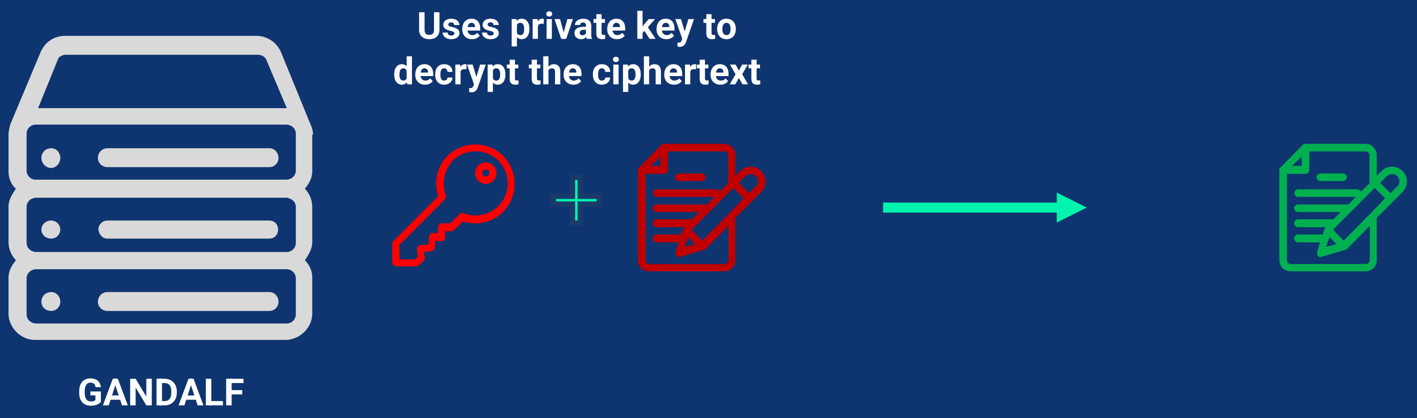


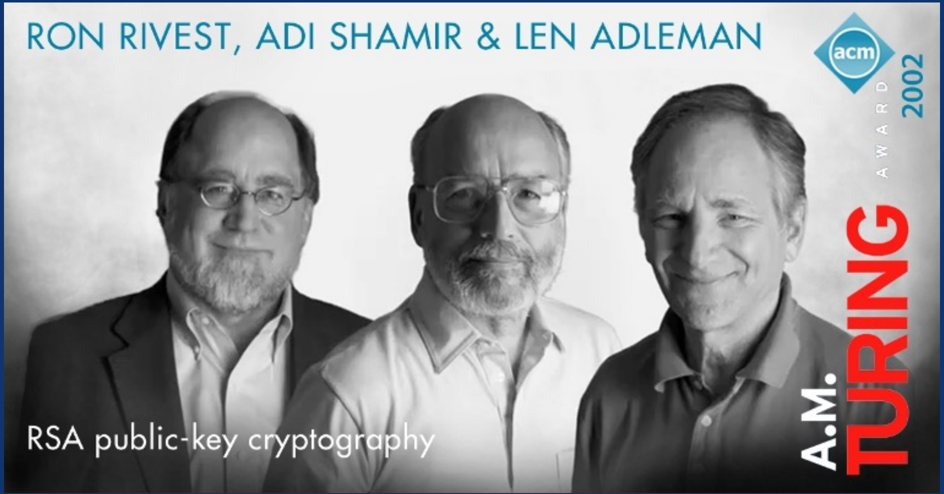
PUBLIC KEY SCHEME

ENCRYPTION

PUBLIC KEY SCHEME

DECRYPTION





RSA CRYPTOSYSTEM

The first famous concretization of Public Key Cryptography. Based on the difficulty of finding the factorization of big integers.

48217917295509614848673267046 7 x 81721434911617336015728474603 7

EASY ↓ DIFFICULT ↑

3940437389838736799380466518880565772525767490583129051892 79

SOME PROBLEMS

- How can we generate a RANDOM key?
- Is Frodo’s message authentic?
- Is the cryptosystem secure? (NO)
- For how long can we reasonably consider a key secure?
- What happens if a key is compromised?

04

GENERATION AND RANDOMNESS

What does it mean *to generate a key (in a secure way)* ?

AN EXAMPLE OF COMPROMISED RANDOMNESS

Sala, M.; Sogiorno, D.; Taufer, D. A Small Subgroup Attack on Bitcoin Address Generation. *Mathematics* 2020, *8*, 1645. https://doi.org/10.3390/math8101645

mathematics

Communication

A Small Subgroup Attack on Bitcoin Address Generation

Massimiliano Sala [1,*], Domenica Sogiorno [2] and Daniele Taufer [3]

1 Department of Mathematics, University of Trento, Via Sommarive 14, 38123 Povo (TN), Italy
2 Department of Mathematics, University of Bari, 70121 Bari, Italy; domenicasogiorno@gmail.com
3 CISPA Helmholtz Center for Information Security, 66123 Saarbrücken, Germany; daniele.taufer@cispa.saarland
* Correspondence: massimiliano.sala@unitn.it

Received: 17 August 2020; Accepted: 21 September 2020; Published: 24 September 2020

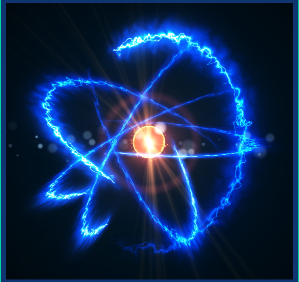
check for updates

Abstract: We show how a small subgroup confinement-like attack may be mounted on the Bitcoin addresses generation protocol, by inspecting a special subgroup of the group associated to point multiplication. This approach does not undermine the system security but highlights the importance of using fair random sources during the private key selection.

COMPUTERS ARE NOT RANDOM

For cryptography we need to generate a lot of unpredictable bits. Any kind of bias can be used by Sauron to improve its attacks

But computers are intrinsically deterministic...



PHYSICS CAN HELP

Physics contains a lot of random phenomena, like radiation or quantum behaviour, that we can manipulate to obtain entropy.
The principal problem is that this processes can be too expensive for some implementations

WE CAN INSTEAD USE PSEUDONUMBER GENERATORS

giacomoborin — magma.exe ◂ magma — 96×19

```
giacomoborin@Giacomos-MacBook-Pro-2 ~ % magma
Magma V2.25-7     Wed Apr 20 2022 11:09:03 on Giacomos-MacBook-Pro-2 [Seed = 2118373592]
Type ? for help.  Type <Ctrl>-D to quit.
> Random(100000000000);
74434094380
> Random(100000000000);
22622629654
> Random(100000000000);
72101417894
>
> SetSeed(2118373592);
>
> Random(100000000000);
74434094380
> Random(100000000000);
22622629654
> Random(100000000000);
72101417894
>
```

https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220

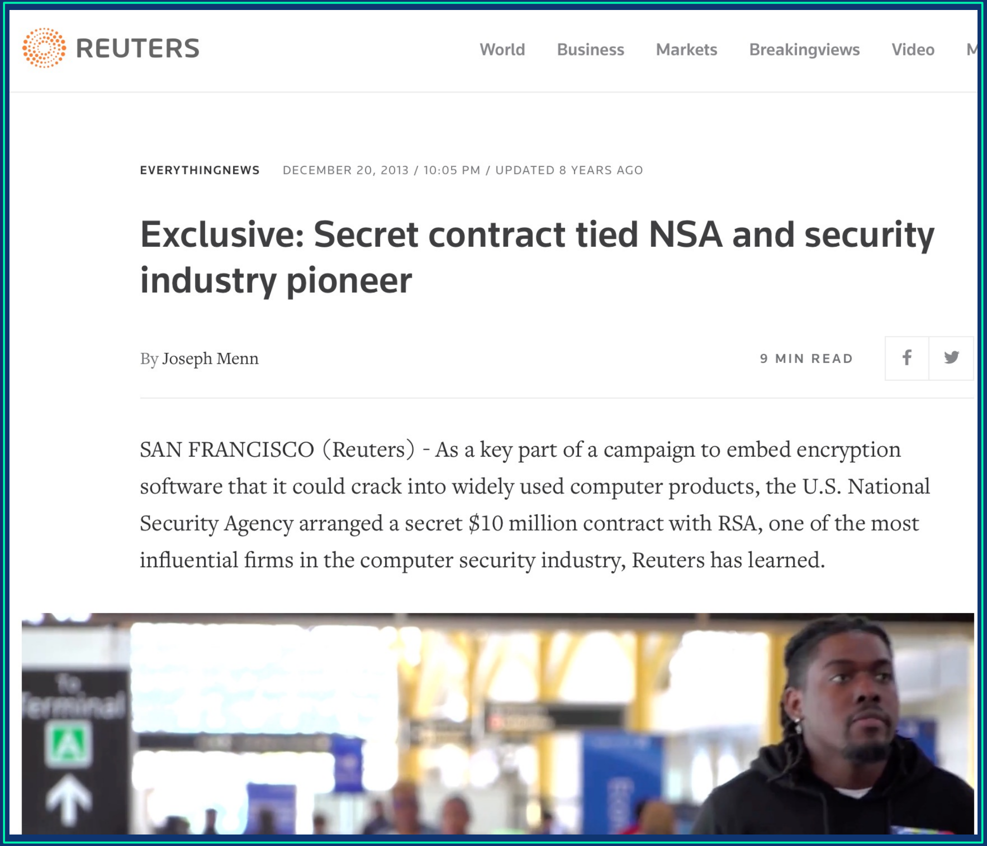
CAN WE TRUST PRNG ?

THE SAD STORY OF DUAL EC DRBG

In 2006 NIST SP 800/90A is published including Dual EC (a PRNG) as standard, ignoring the warnings of the cryptographic community.

In 2007 Dan Shumow and Niels Ferguson proved that it was possible that the designers of Dual EC inserted a backdoor to recover the seed from some of the values.

In 2013 information leaked by Snowden showed that NSA is the designer of Dual EC



REUTERS

World Business Markets Breakingviews Video

EVERYTHINGNEWS DECEMBER 20, 2013 / 10:05 PM / UPDATED 8 YEARS AGO

Exclusive: Secret contract tied NSA and security industry pioneer

By Joseph Menn

9 MIN READ

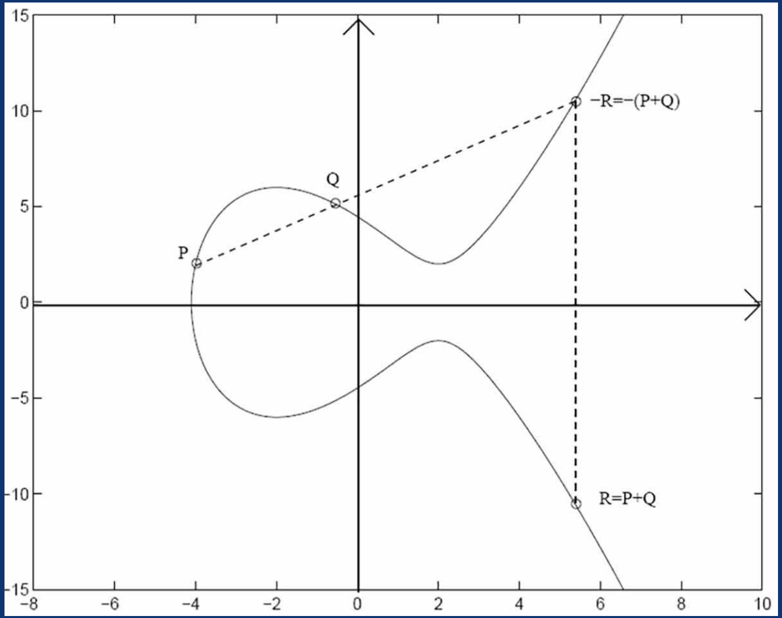
SAN FRANCISCO (Reuters) - As a key part of a campaign to embed encryption software that it could crack into widely used computer products, the U.S. National Security Agency arranged a secret $10 million contract with RSA, one of the most influential firms in the computer security industry, Reuters has learned.

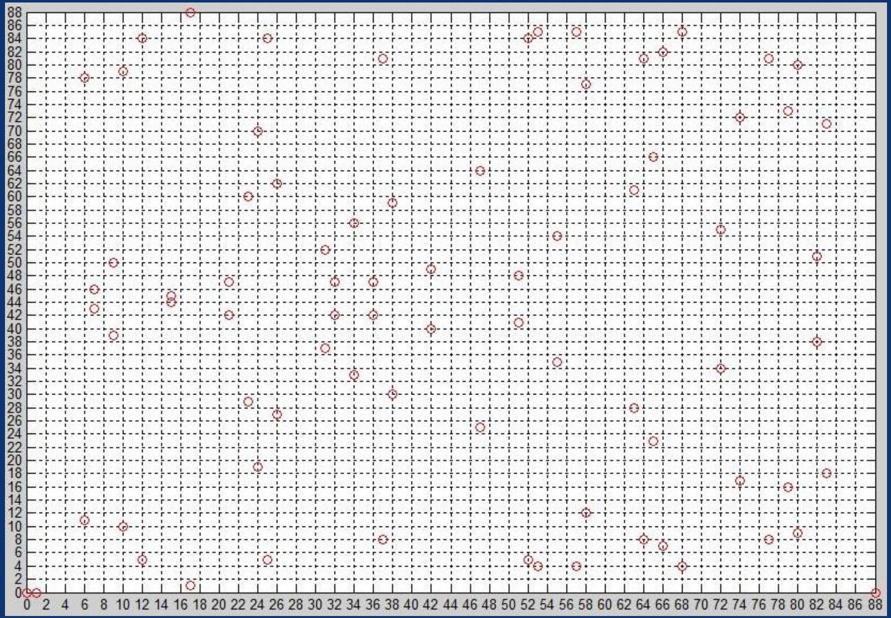
Article : Government Announces Steps to Restore Confidence on Encryption Standards by NICOLE PERLROTH on The New York Times link : https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/

But internal memos leaked by a former N.S.A. contractor, Edward Snowden, suggest that the N.S.A. generated one of the random number generators used in a 2006 N.I.S.T. standard — called the Dual EC DRBG standard — which contains a back door for the N.S.A. In publishing the standard, N.I.S.T. acknowledged "contributions" from N.S.A., but not primary authorship.

Internal N.S.A. memos describe how the agency subsequently worked behind the scenes to push the same standard on the International Organization for Standardization. "The road to developing this standard was smooth once the journey began," one memo noted. "However, beginning the journey was a challenge in finesse."

SMALL DIGRESSION: ELLIPTIC CURVES





Elliptic curve y^2=x^3-x on finite field Z 89
(From Wikipedia)

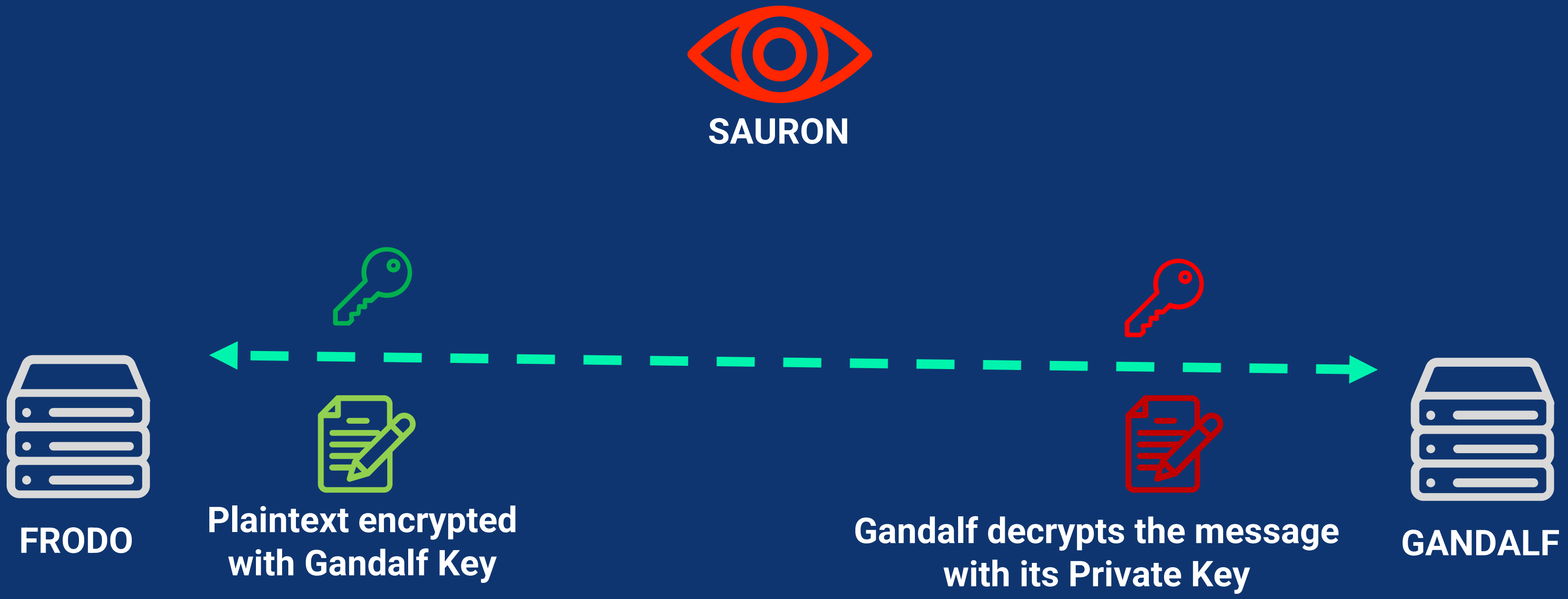
05

AUTHENTICATION

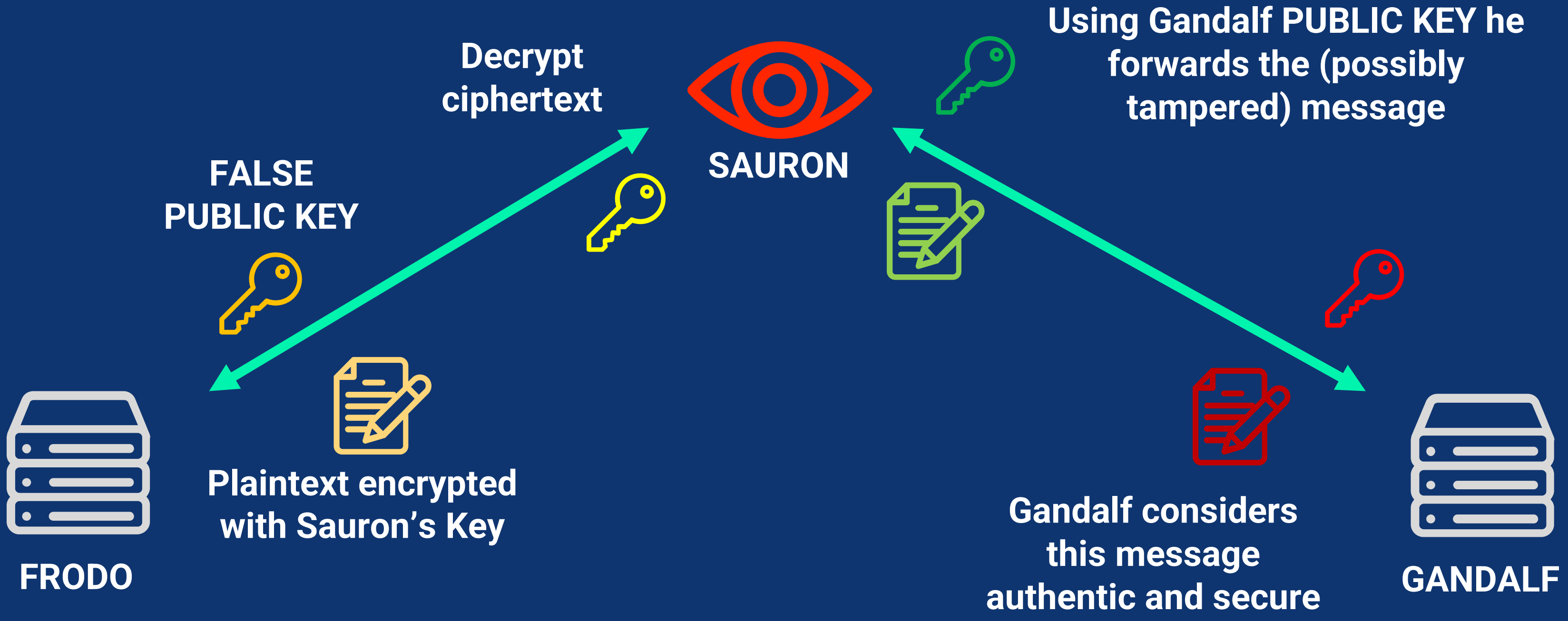
How can Frodo prove his identity?

MAN IN THE MIDDLE ATTACK

WHAT THEY THINK ARE DOING

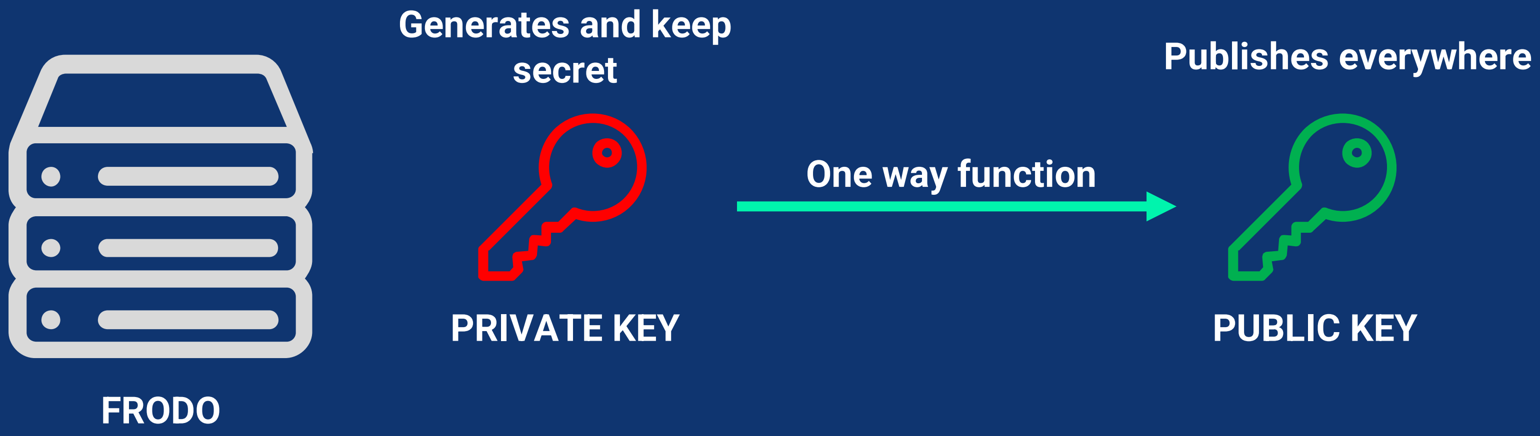


MAN IN THE MIDDLE ATTACK
WHAT IS HAPPENING



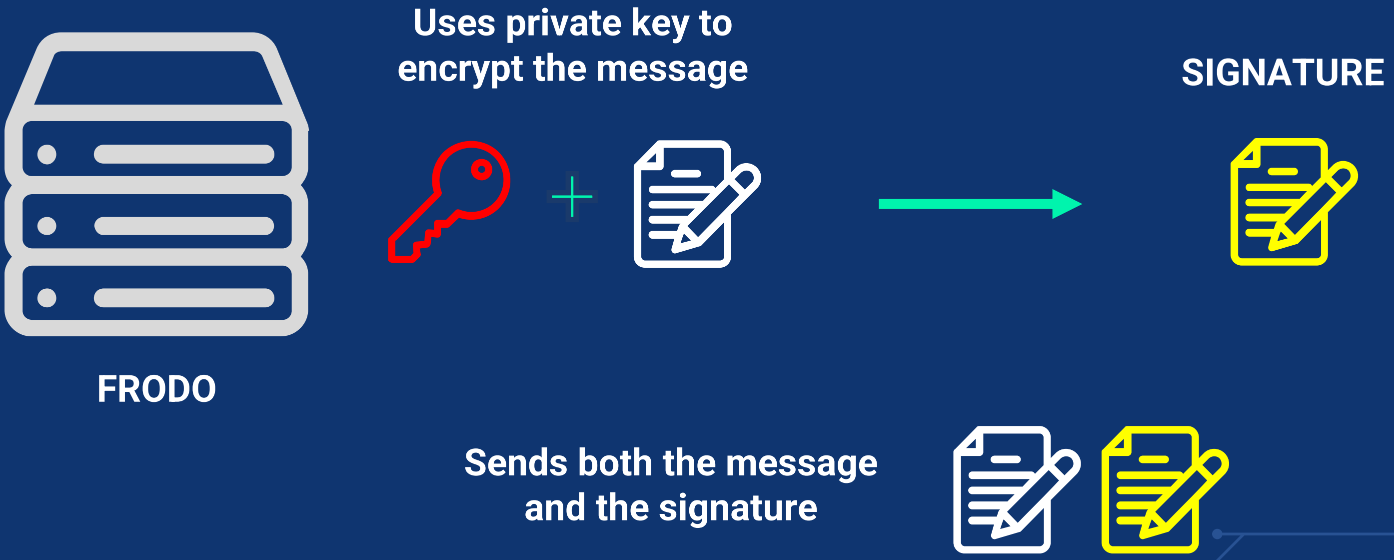
DIGITAL SIGNATURE SCHEME

CREATION OF THE KEYS (SAME AS PUBLIC KEY SCHEME)



DIGITAL SIGNATURE SCHEME

SIGNATURE CREATION



DIGITAL SIGNATURE SCHEME

SIGNATURE VERIFICATION

Sadly the problem persists, Sauron can again repeat Man In the Middle to forge a signature

WE NEED TO BIND TOGETHER

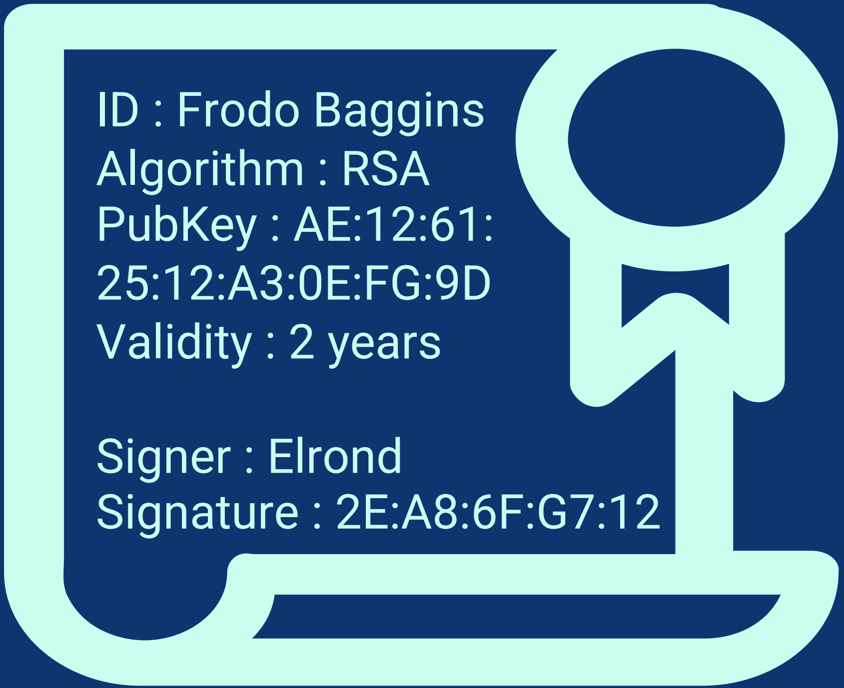
IDENTIY

PUBLIC KEY

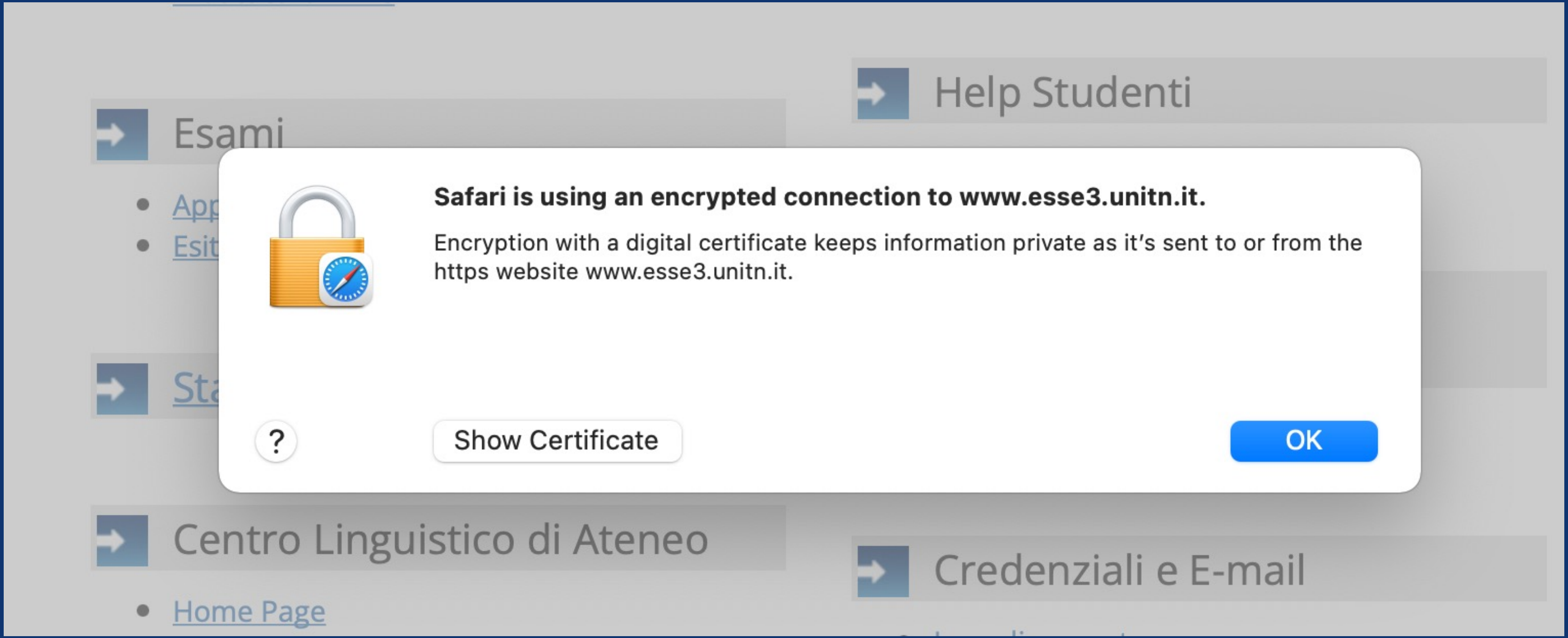
Can we physically exchange them?
Not really, not scalable and unusable

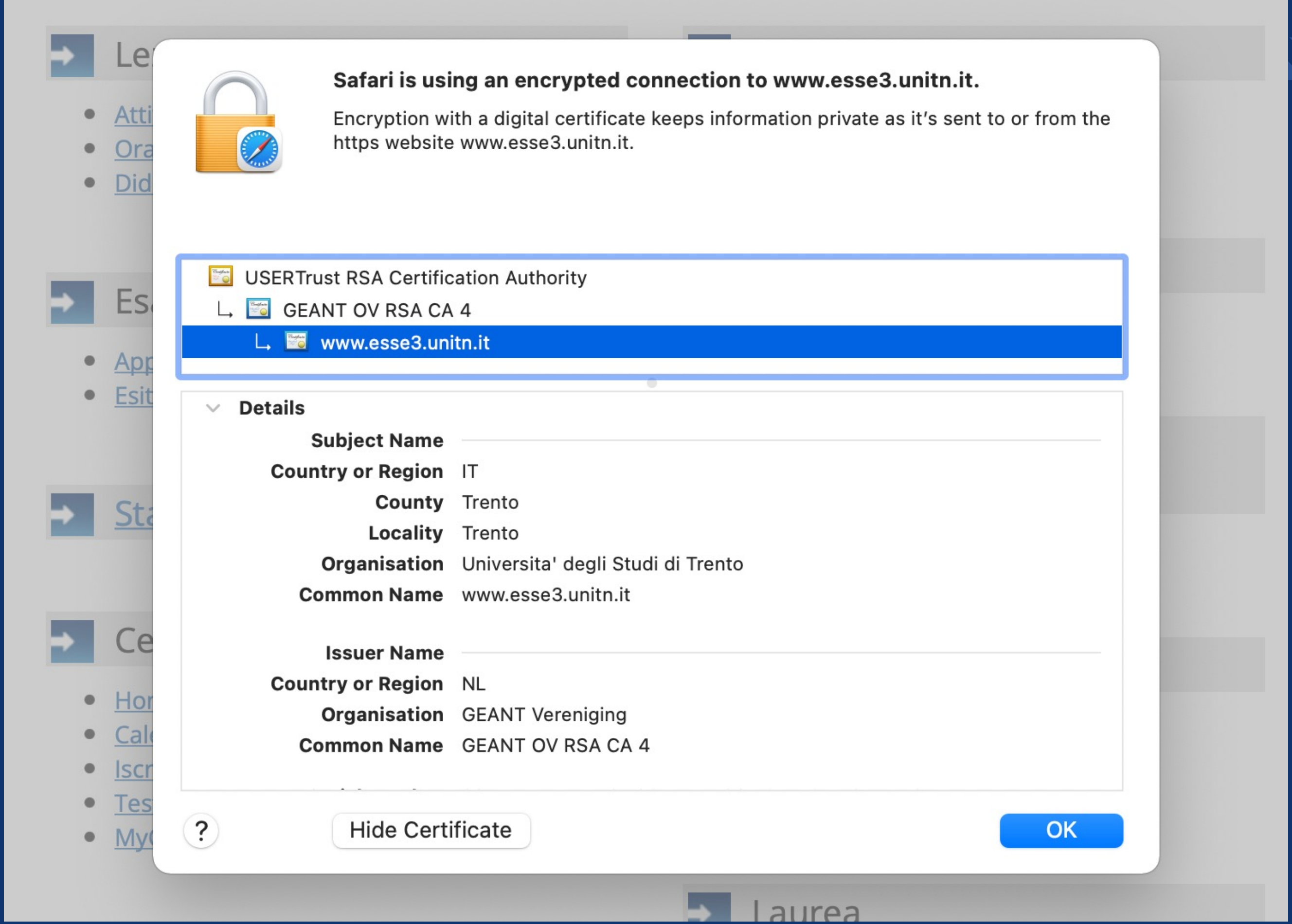
PUBLIC KEY INFRASTRUCTURE

1. We all agree in trusting a central authority (ELROND) with its public key
2. Elrond verifies the identity of a user (FRODO)
3. Then Elrond creates a certificate containing Frodo's public key and signs it with its private key
4. Frodo can exhibit the certificate to receive or sign messages



AN EXAMPLE


Help Studenti
Esami
Centro Linguistico di Ateneo
Home Page
Credenziali e E-mail
Safari is using an encrypted connection to www.esse3.unitn.it.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.esse3.unitn.it.
?
Show Certificate
OK


Safari is using an encrypted connection to www.esse3.unitn.it.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.esse3.unitn.it.
USERTrust RSA Certification Authority
GEANT OV RSA CA 4
www.esse3.unitn.it
Details
Subject Name
Country or Region IT
County Trento
Locality Trento
Organisation Universita' degli Studi di Trento
Common Name www.esse3.unitn.it
Issuer Name
Country or Region NL
Organisation GEANT Vereniging
Common Name GEANT OV RSA CA 4
?
Hide Certificate
OK
Laurea

Issuer Name	
Country or Region	NL
Organisation	GEANT Vereniging
Common Name	GEANT OV RSA CA 4
Serial Number	00 BA EA FF 58 61 C2 EF E3 C0 52 FA 27 AC D8 56 47
Version	3
Signature Algorithm	SHA-384 with RSA Encryption (1.2.840.113549.1.1.12)
Parameters	None
Not Valid Before	Friday, 30 April 2021 at 02:00:00 Central European Summer Time
Not Valid After	Sunday, 1 May 2022 at 01:59:59 Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	384 bytes: AF 72 8D D8 7E 6B 52 8E 24 DE 9B EF 0B 0D 8F 17 CB 07 B8 A7 8D 0A 81 ED 9C 41 FB 38 B1 E3 67 39 C7 37 87 FE 56 31 3D F7 3D A1 68 7E 22 20 D5 8F 95 53 8D 73 D9 EB 71 D5 EE C3 F2 18 1C 26 4B B2 92 9F 0E B7 DD DC 11 F9 3E 2D A5 30 7D 89 22 1C 0E …
Exponent	65537
Key Size	3.072 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes: 22 AF B0 17 1D 08 4C CC F3 1F B8 BD A0 FD 27 9C 8A 40 3A EA 51 9A EA 96 62 60 3A D5 09 94 12 C1 48 81 25 FF 07 60 93 E2 AA EE C1 C6 E0 5E 7B AA 2A 93 C5 41 C7 4A 62 BE BE 74 8D 0A 03 8F 45 AD E4 25 07 ED 35 C7 E5 15 3F 10 E8 2F AC ED E6 B0 CB …

06

POST QUANTUM CRYPTOGRAPHY

For how long will we be safe?

WHAT IS A QUANTUM COMPUTER?

Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

Quoted from ibm.com/topics/quantum-computing

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability

TO MAKE A LONG STORY SHORT WE CAN REDUCE A SUB-EXPONENTIAL COMPLEXITY TO A POLYNOMIAL ONE

COMPARISON OF COMPLEXITY

NUMBER TO FACOTR	814821397503009018584246798958336355437610311235778760412223468062833704983773390162893111848984955782536216161904479266508474835953444051721939789557
EXPECTED OPERATIONS FOR BRUTE FORCE	1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
EXPECTED OPERATIONS FOR NUMBER FIELD SIEVE	100000000000000000000000000000000000000000000000000
SHOR'S ALORITHM	125000000
SECONDS FROM THE BIG BANG	434700000000000

You can read something more here: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

HACKERS SAVING ENCRYPTED DATA

Article seen in Applied Cryptography lectures (Prof. Silvio Ranise)
link : technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

MIT Technology Review

Featured Topics Newsletters Events Podcasts

Sign in Subscribe

COMPUTING

The US is worried that hackers are stealing data today so quantum computers can crack it in a decade

The US government is starting a generation-long battle against the threat next-generation computers pose to encryption.

By Patrick Howell O'Neill

November 3, 2021

NP COMPLETE PROBLEMS

Intuitive definition

A decision problem is NP-complete if:

- There exists some piece of information that allow us to quickly verify if it exists a solution (*NP, i.e. solvable by a Non-Deterministic Turing Machine in Polynomial Time*)
- It is at least as hard as any other NP problem (*NP-Hard, i.e. there exists a polynomial reduction to another NP-complete problem*)

Example

Boolean satisfiability problem (SAT) : given a Boolean expression decide if there exists an interpretation that satisfies it :

For

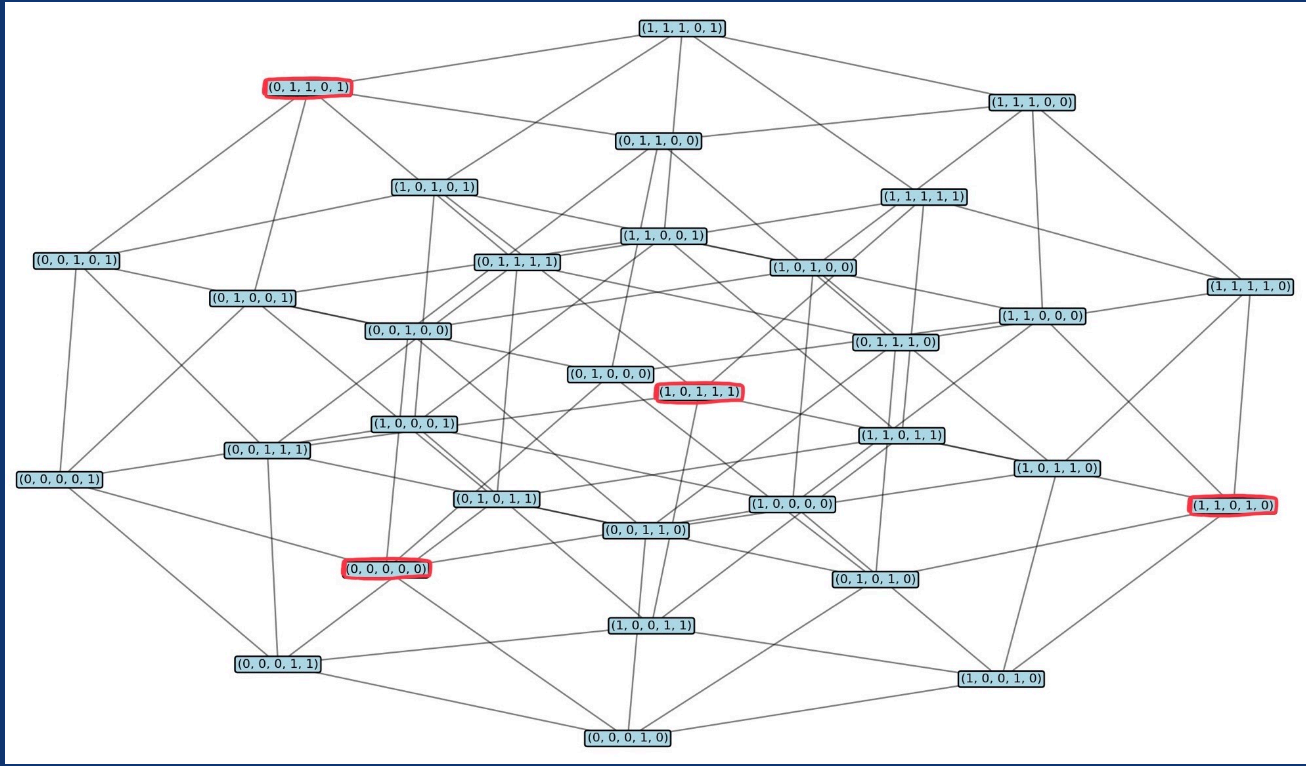
“`(p or q or f) and (f or not p)`”

it exists, one possible is

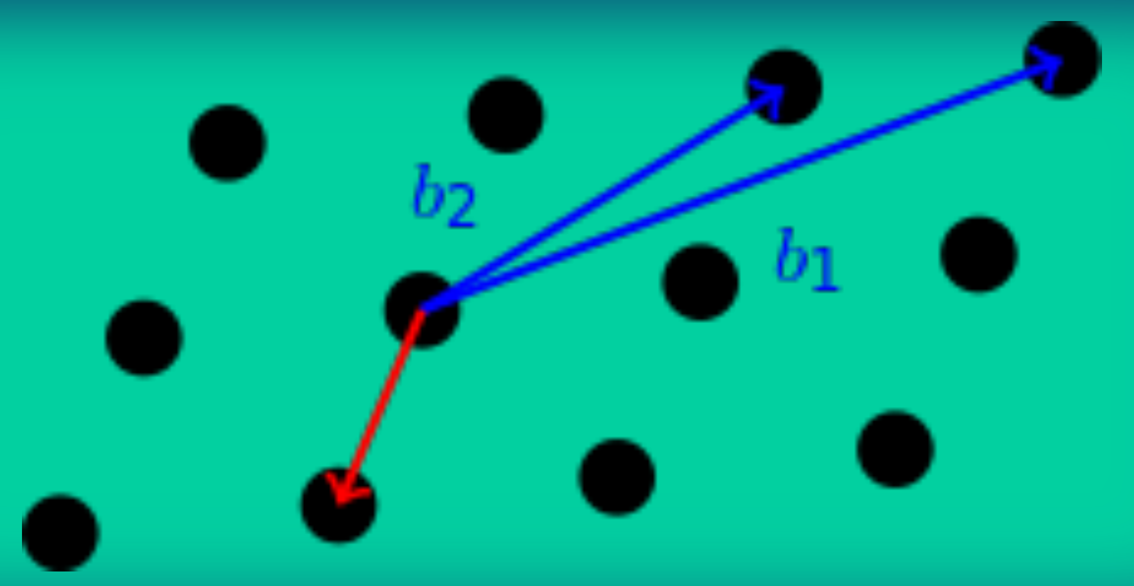
p = q = FALSE, f = TRUE. ⟵ VERIFIER

SEEMS LIKE NP-COMPLETE PROBLEMS RESIST TO ATTACKS FROM QUANTUM COMPUTERS

NEAREST CODEWORD PROBLEM



SHORTEST VECTOR PROBLEM



NEW NIST CALL FOR PQ STANDARDIZATION

HTTPS://CSRC.NIST.GOV/PROJECTS/POST-QUANTUM-CRYPTOGRAPHY

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PROJECTS

Post-Quantum Cryptography PQC

Overview

Post-Quantum Encryption:
A Q&A With NIST's Matt Scholl

Post-Quantum Cryptography: the Good, the Bad, and the Powerful (video)

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. **Full details can be found in the Post-Quantum Cryptography Standardization page.**

PROJECT LINKS

Overview

FAQs

News & Updates

Events

Publications

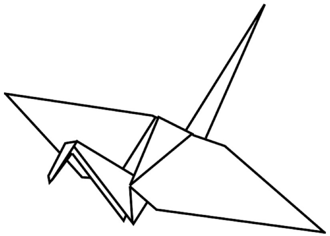
Presentations

A PROPOSE FROM ITALY : LEDACRYPT

LEDAcrypt *(merger of LEDAkem and LEDApkc)*	Zip File (2MB) KAT Files (47MB) IP Statements Website	Marco Baldi Alessandro Barenghi Franco Chiaraluce Gerardo Pelosi Paolo Santini

LEDAcrypt: Low-dEnsity parity-check coDe-bAsed cryptographic systems

Specification revision 3.0 – April, 2020



Based on linear coding theory (QC LDPC Codes)
It reached round 2 of standardization, but not round 3

INIZIATIVA NAZIONALE
DE COMPONENDIS CIFRIS

If you are interested in Cryptography, you can find a lot of material here:
decifris.it or
linkedin.com/in/de-componendis-cifris-iniziativa-nazionale-8274501a5/
It is the Italian association for the promotion of cryptography. They propose events, seminaries, scholarships and more.

THANKS!

Do you have any questions?

giacomo.borin@studenti.unitn.it
giacomoborin.github.io