A brief introduction to provable security

Guillaume Scerri

10 november, 2025

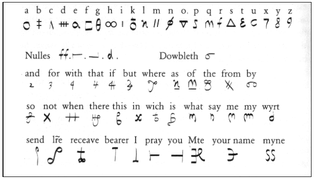
Table of Contents

A brief history of cryptography

Historically: secret process

invisible ink, set of abbreviations

Problem: once someone knows your process, everything is broken.
See Mary Stuart:



a b c d e f g h i k l m n o p q r s t u x y z

Nulles ff. — . — . d . Dowbleth σ

and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lre receave bearer I pray you Mte your name myne

Kerckhoff's principle (1)

La Cryptographie Militaire (1883)

Le système doit être matériellement,
sinon mathématiquement, indéchiffrable

The system should be, if not theoretically unbreakable,
unbreakable in practice

$\longrightarrow$ If the security cannot be formally proven,
heuristics should provide some confidence.

Kerckhoffs' Principles (2)

La Cryptographie Militaire (1883)

Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi

Compromise of the system should not inconvenience the correspondents

$\longrightarrow$ The description of the mechanism should be public

Kerckhoffs' Principles (3)

La Cryptographie Militaire (1883)

La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants

The key should be rememberable without notes and should be easily changeable

$\longrightarrow$ The parameters specific to the users (the key) should be short

During the second world war

Cryptography becomes a mathematical process: small key, code books, does not (in theory) rely on secrecy of process

Decrypted by Alan Turing, with access to machines. Unclear assumptions for security.

Modern days

RSA, AES, ECDSA, ...

- Public specifications/implementation, standardised, largely studied
- Often standardised (mostly by NIST)
- Largely studied by researchers

Assumptions

In this course we assume cryptography is secure (will see what it means later).

Usual cryptographic primitives (1)

Symmetric encryption:

- ex. AES
- One key, secret, shared by both parties
- Very efficient
- Key distribution?
- Secrecy of ciphertext if key unknown

Asymmetric encryption:

- ex. RSA
- Public/private key pair
- Somewhat inefficient
- Secrecy of ciphertext if private key unknown

Usual cryptographic primitives (2)

Signatures :

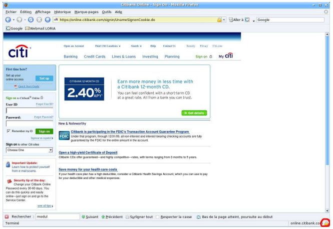
- ex. RSA
- Verifying/signing key pair
- Anyone can verify a signature (with verifying key)
- Producing valid signature requires signing key.

Random numbers (nonces) :

- Uniformly drawn bitstring
- Should be “hard” to guess
- Used as challenges, seeds for keys (or key pairs).

Table of Contents

Where do we need security?


Citibank Online - Sign On - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils Aide
https://online.citibank.com/signin/UnameSignonCookie.do
Google Webmail LORIA
Open an Account Find Citi Locations Search Help Contact Us Security Privacy Citi.com
Banking Credit Cards Lines & Loans Investing Planning Sign on My Citi
Set up
Quick Start Guide
Forgot User ID?
Forgot Password?
Sign on
Ingresar en español
Choose One
Get details
see all tips
Rechercher : modul Suivant Précédent Surligner tout Respecter la casse Bas de la page atteint, poursuite au début
Terminé
online.citibank.com

First time here?
Set up your online access

Sign on to Citibank® Online
User ID
Password:
Remember my ID

Sign on to other Citi sites

CITIBANK 12-MONTH CD
2.40% APY

Earn more money in less time with a Citibank 12-month CD.
You can feel confident with a short-term CD at a great rate. All from a bank you can trust.

New & Noteworthy

Citibank is participating in the FDIC's Transaction Account Guarantee Program
Under that program, through 12/31/09, all non-interest and interest-bearing checking accounts are fully guaranteed by the FDIC for the entire amount in the account.

Open a high-yield Certificate of Deposit
Citibank CDs offer guaranteed—and highly competitive—rates, with terms ranging from 3 months to 5 years.

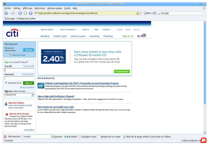
Save money for your health care costs
If your health care plan has a high deductible, consider a Citibank Health Savings Account, which you can use to pay for your deductible and other medical expenses.

Important Update:
Learn how to protect yourself from e-mail scams.

Security tip of the day:
Change your Citibank Online Password every 30-60 days. You can do this quickly and easily online—just sign on and go to the Service Center.

What do we expect from Security?

- Keep the PIN code secret



- Ensure integrity of data

- Ensure that tally is correct

A simple example

Let's assume you want to connect to your bank's website.

What are you expecting in terms of security?

A simple example

Let's assume you want to connect to your bank's website.

What are you expecting in terms of security?

- Know that you are talking to your bank
- Secret communication
- ...

Goes beyond what crypto immediately ensures !

Against whom ?

- Malicious and powerful attacker
- hence not a simple correctness problem
  $\Rightarrow$ need for formal verification !

Formal verification

For P protocol and ϕ security property:

$\forall$ $\in \mathcal{C}$ $\quad$ $P \|$ $\models^{?} \phi$

- What is P?
- What is ϕ?
- *What is $\mathcal{C}$?*

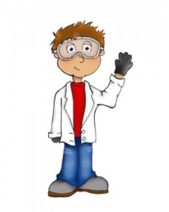
An example of protocol

Alice wants to send N_a to Bob.
Cryptographic primitive: asymmetric encryption

key pair pk public encryption key, sk secret decryption key

$$\xrightarrow{a,\{N_a\}_{pk_b}}$$

$$\xleftarrow{\{N_a\}_{pk_a}}$$



What is P

- Set of agents
- That communicate on a network

Protocol algebra

We need to define a protocol algebra and its semantics. Should contain:

- input/outputs from the network;
- reasonable computations, tests and branching on received messages;
- parallel composition of agents;
- (probably) arbitrary replication of an agent.

An example of protocol (ctd.)

Alice wants to send N_a to Bob.
Cryptographic primitive: asymmetric encryption
key pair pk public encryption key, sk secret decryption key

$$\xrightarrow{a,\{N_a\}_{pk_b}}$$

$$\xleftarrow{\{N_a\}_{pk_a}}$$

Security properties:

- N_a should be secret
- If Alice accepts Alice and Bob should agree on N_a

Language for security properties

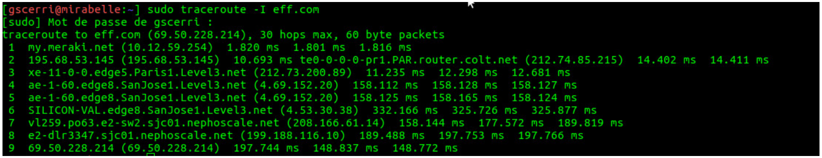
Should be able to express (at the very least):

- Secrecy of values;
- Agreement of agents on some values.

We need a simple logic on events that happen in the protocol!

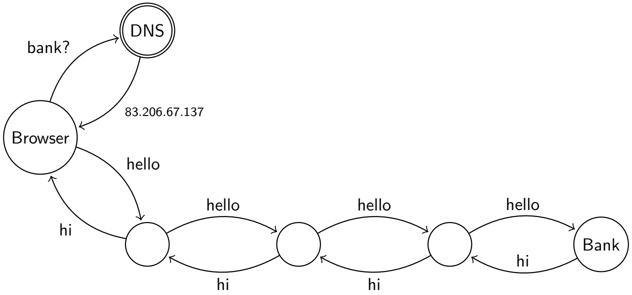
Attacker capabilities: network

Type url in address bar and this happens:



```
[gscerri@mirabelle:~] sudo traceroute -I eff.com
[sudo] Mot de passe de gscerri :
traceroute to eff.com (69.50.228.214), 30 hops max, 60 byte packets
 1  my.meraki.net (10.12.59.254)  1.820 ms  1.801 ms  1.816 ms
 2  195.68.53.145 (195.68.53.145)  10.693 ms te0-0-0-0-pr1.PAR.router.colt.net (212.74.85.215)  14.402 ms  14.411 ms
 3  xe-11-0-0.edge5.Paris1.Level3.net (212.73.200.89)  11.235 ms  12.298 ms  12.681 ms
 4  ae-1-60.edge8.SanJose1.Level3.net (4.69.152.20)  158.112 ms  158.128 ms  158.127 ms
 5  ae-1-60.edge8.SanJose1.Level3.net (4.69.152.20)  158.125 ms  158.165 ms  158.124 ms
 6  SILICON-VAL.edge8.SanJose1.Level3.net (4.53.30.38)  332.166 ms  325.726 ms  325.877 ms
 7  vl259.po63.e2-sw2.sjc01.nephoscale.net (208.166.61.14)  158.144 ms  177.572 ms  189.819 ms
 8  e2-dlr3347.sjc01.nephoscale.net (199.188.116.10)  189.488 ms  197.753 ms  197.766 ms
 9  69.50.228.214 (69.50.228.214)  197.744 ms  148.837 ms  148.772 ms
```

Attacker capabilities: network ctd.



What could possibly go wrong?

No security at network layer

- DNS poisoning
- message interception
- wiretapping

Needham-Schroeder (1978)

“We assume that the intruder can interpose a computer in all communication paths, and thus can alter or copy parts of messages, replay messages, or emit false material. While this may seem an extreme view, it is the only safe one when designing authentication protocols.”

Attacker

- Untrusted network: controls the network
- Able to compute: can modify messages

Computations

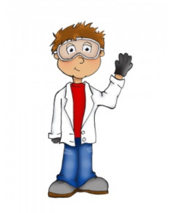
Adversarial computations are the most important parameter of what we prove, a number of computation models exist, we will spend a lot of time on this point!

A simple attack

Alice wants to send a N_a to Bob.

$$\xrightarrow{a,\{N_a\}_{pk_b}}$$

$$\xleftarrow{\{N_a\}_{pk_a}}$$

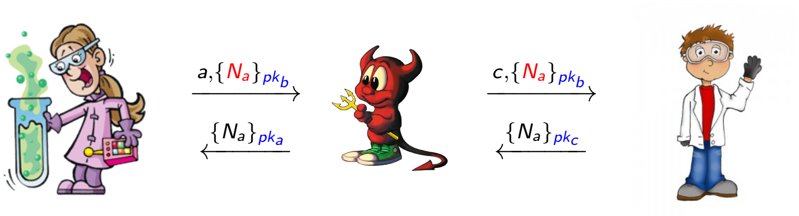


Security properties:

- N_a should be secret
- If Alice accepts Alice and Bob should agree on N_a

A simple attack

Alice wants to send a N_a to Bob.



Security properties:

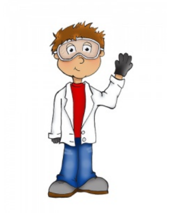
- N_a should be secret
- If Alice accepts Alice and Bob should agree on N_a

A simple attack

Alice wants to send a N_a to Bob.

$$\xrightarrow{\{a,N_a\}_{pk_b}}$$

$$\xleftarrow{\{N_a\}_{pk_a}}$$



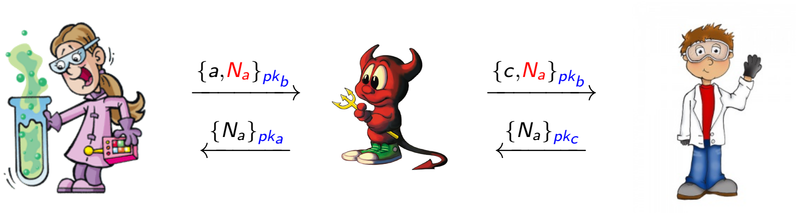
Security properties:

- N_a should be secret
- If Alice accepts Alice and Bob should agree on N_a

Computations matter!

With an El Gamal encryption (with some hypotheses on the implementation of $\langle \cdot, \cdot \rangle$) we have

$$\{a, N_a\}_{pk_b} \times \frac{c}{a} = \{c, N_a\}_{pk_b}$$



Is it an attack?

It depends, we need to be careful about our model of adversarial computations and its adequation with primitives!

What we do not consider in this course

- Side channel attacks
  $\Rightarrow$ we only care about the input/output semantics of computation not possible side effects
- System aspects (viruses, bad OS, ...)
  agents are either dishonest or behave perfectly honestly

Table of Contents

Outline

1. Definition of a generic process algebra
    - Model concurrency aspects.
    - Leave adversarial computations as a parameter.
    - Give a small language for security properties.
2. Symbolic model of cryptography
    - Definition of a term algebra based computation semantics.
    - Decidability of security for bounded protocols.
    - Modelling unbounded protocols and proof strategies (hopefully).
3. Computational model of cryptography.
    - Definition of a poly-time Turing Machine computation semantics.
    - Modelling computational security of primitives .
    - A brief introduction to game based proofs.