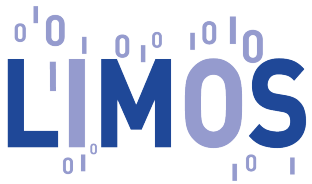
Introduction to Cryptography

Pascal Lafourcade

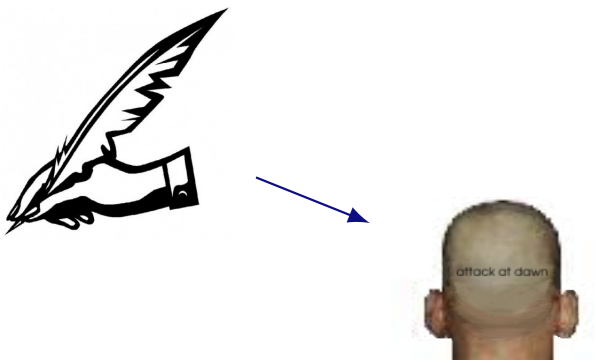


ESC January 2021

Outline

Art to hide written secret

Art to hide written secret



Steganography

Art to hide written secret

Cryptography

Steganography

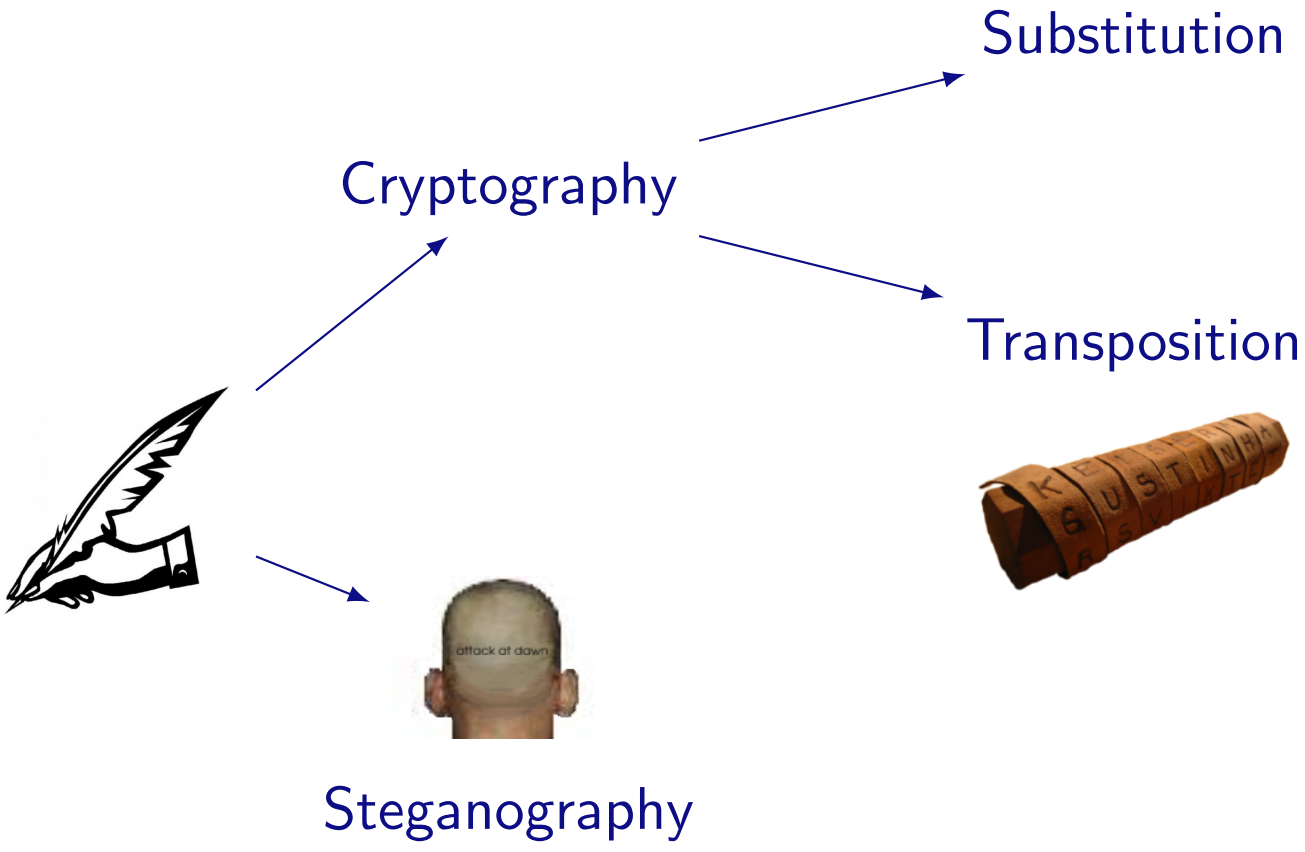
Art to hide written secret

Cryptography

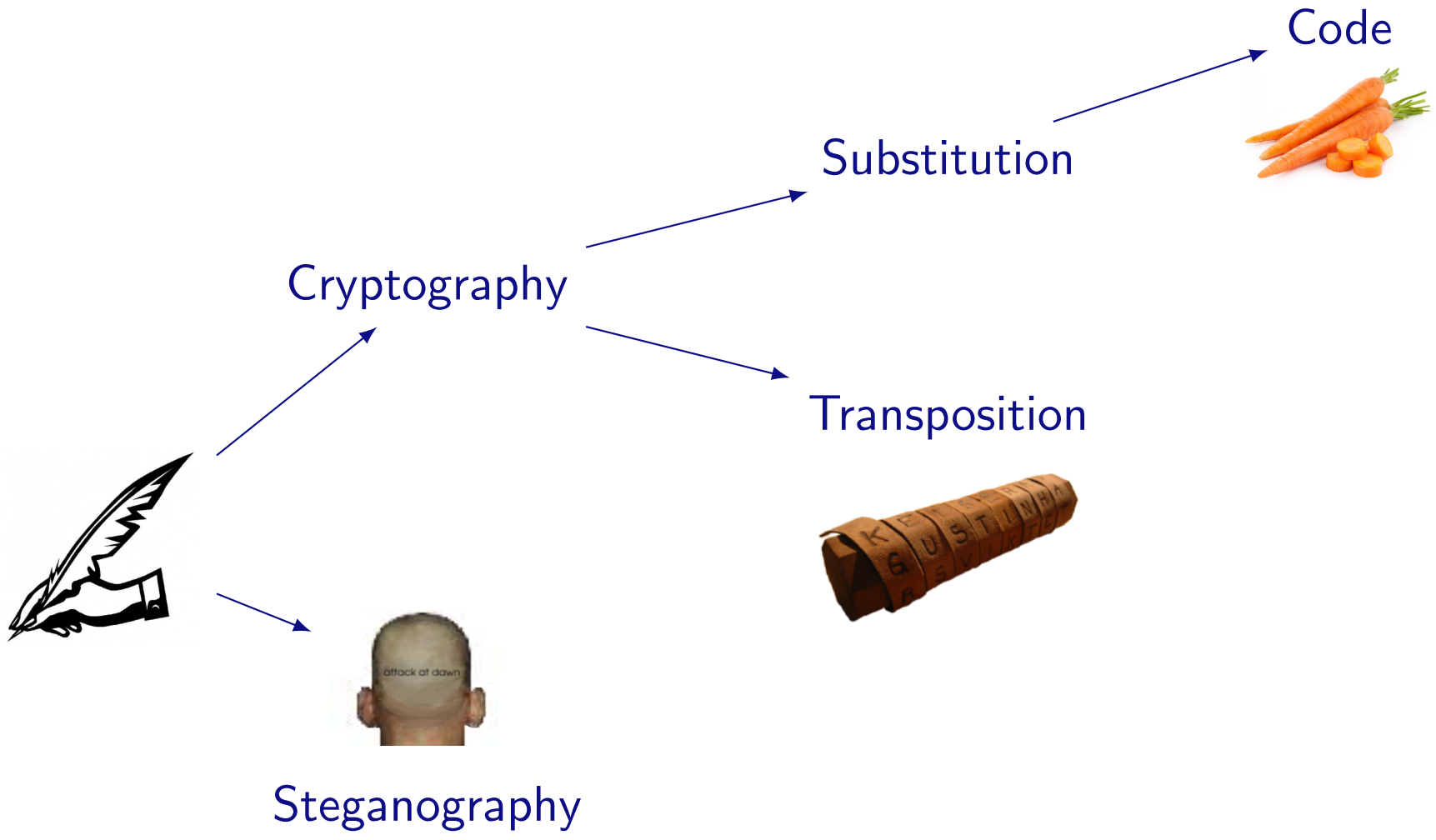
Transposition

Steganography

Art to hide written secret



Art to hide written secret



Art to hide written secret

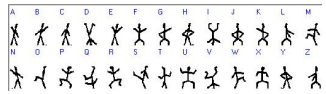
Cryptography

Steganography

Substitution

Code

Encryption



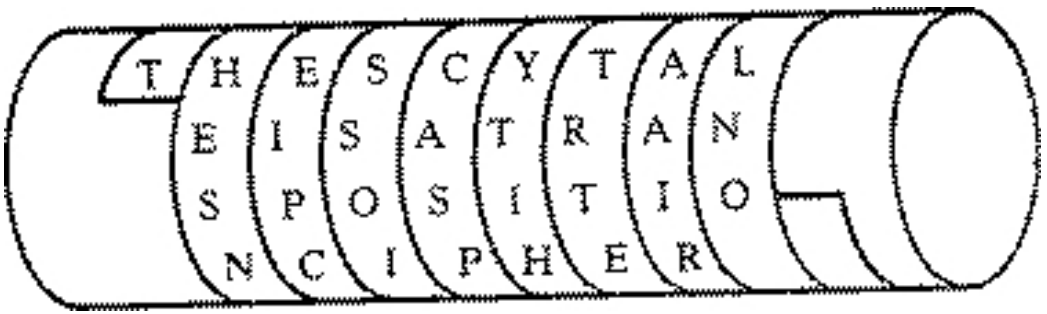
Transposition

Applications

Long time ago

Grecks and Scythale

Grecks and Scythale



Transposition

Romans

Caesar Encryption
Substitution +3

Romans

Caesar Encryption
Substitution +3

Dyh Fhvdu

Romans

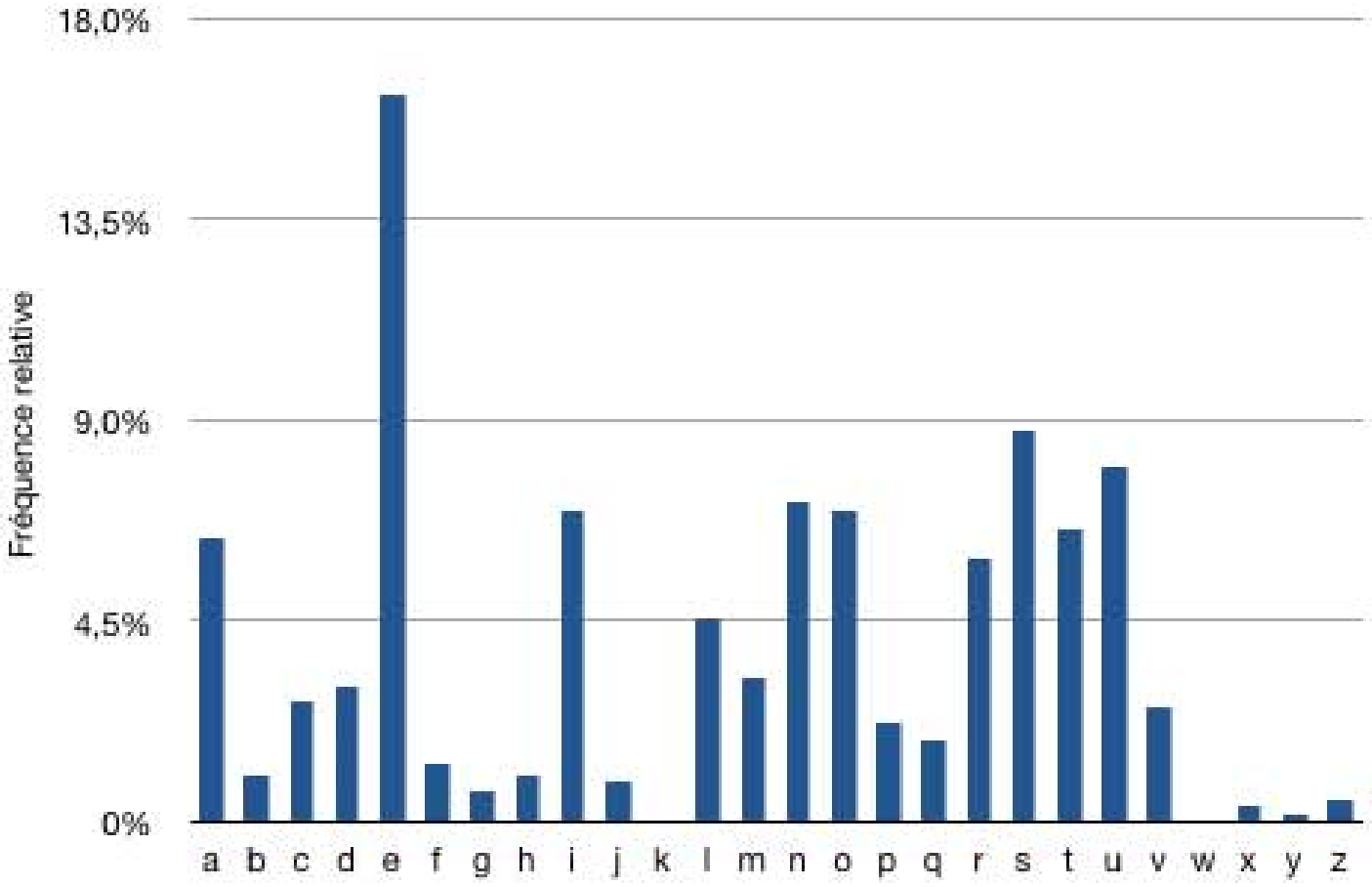
Caesar Encryption
Substitution +3

Dyh Fhvdu

Ave Cesar

Is it secure ?

Is it secure ?



Frequence Analysis

Substitution polyalphabetic (Alberti, Vigenère 1553)

Example with the key k = 3,7,10

m = CON NAI TRE

Substitution polyalphabetic (Alberti, Vigenère 1553)

Example with the key k = 3,7,10

$$m = \text{CON NAI TRE}$$

$$E_k(m) = \text{FVX QHS WYO}$$

Kerchoff's Principle

In 1883, a Dutch linguist Auguste Kerchoff von Nieuwenhof stated in his book "La Cryptographie Militaire" that:

"the security of a crypto-system must be totally dependent on the secrecy of the key, not the secrecy of the algorithm."

Author's name sometimes spelled Kerckhoff

Encryption : Enigma (Second World War)


+

=

Encryption : Enigma (Second World War)

Encryption : Enigma (Second World War)


+

=

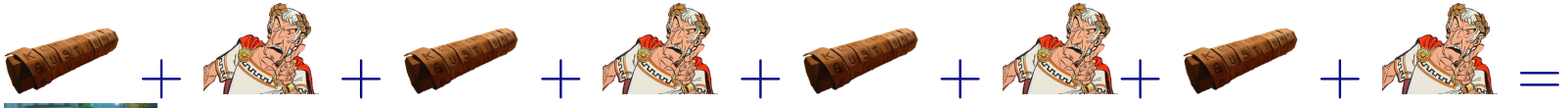


+

=

Encryption : Enigma (Second World War)

Encryption : Enigma (Second World War)



One-Time Pad (Vernam 1917)

Example:

$$\begin{array}{rcl} m & = & 010111 \\ k & = & 110010 \\ \hline c & = & 100101 \end{array}$$

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Principle

A good cipher design uses Confusion and Diffusion together

Outline

c

o

n

c

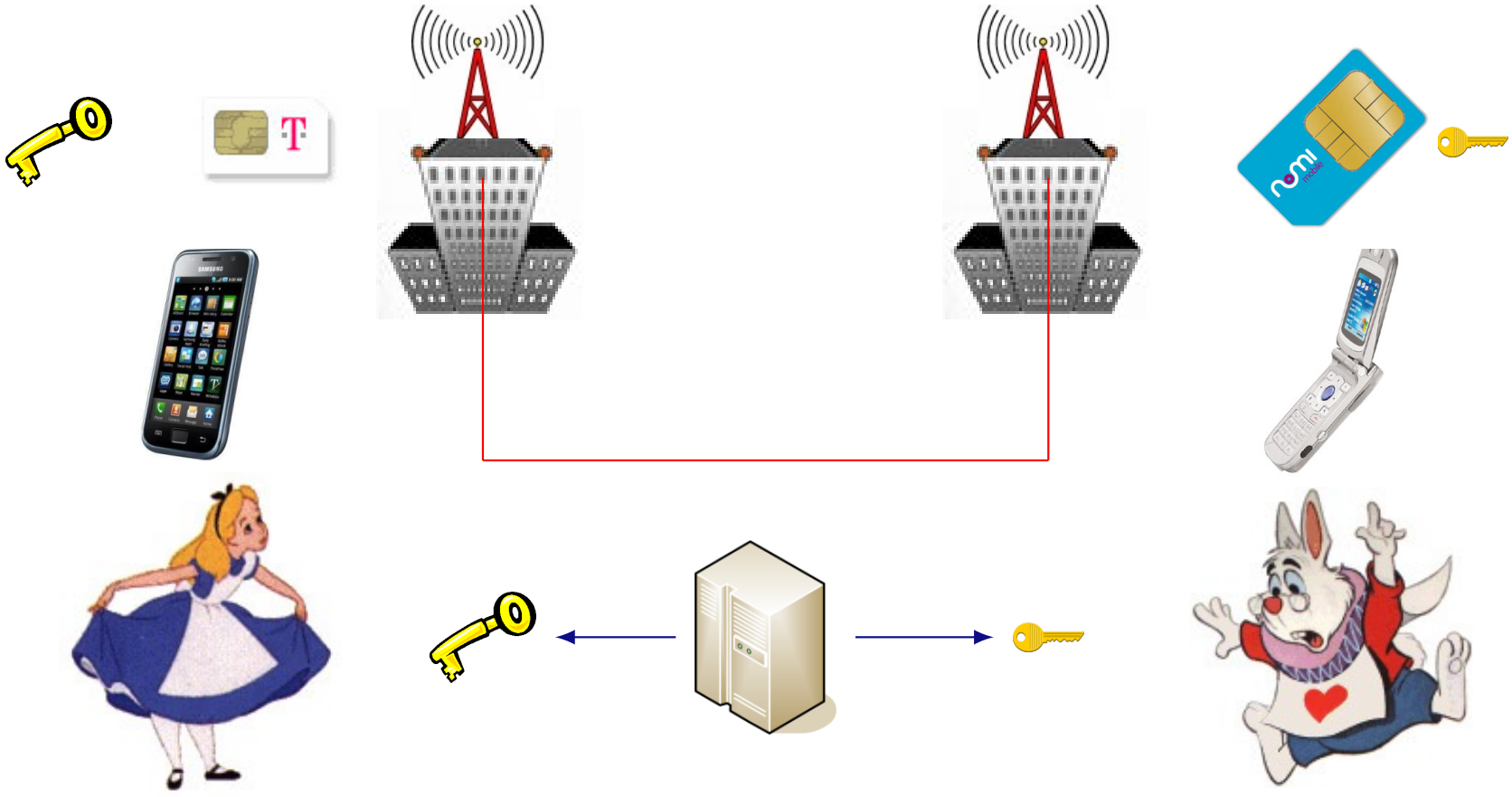
l

Symmetric Encryption

Examples

- Caesar, Vigenère
- One Time Pad (OTP) $c = m \oplus k$
- Data Encryption Standard (DES) 1976
- Advanced Encryption Strandard (AES) 2001

Phone Communications



Public Key Encryption

Examples

- RSA (Rivest Shamir Adelmman 1977): $c = m^e \mod n$
- ElGamal (1981) : $c \equiv (g^r, h^r \cdot m)$

Comparaison

- Size of the key
- Complexity of computation (time, hardware, cost ...)
- Number of different keys ?
- Key distribution
- Signature only possible with asymmetric scheme

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

	DVD 4,7 G.B		Blu-Ray 25 GB	
Schemes	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

ElGamal Encryption Scheme

Key generation: Alice chooses a prime number p and a group generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.

Public key: (p, g, h), where $h = g^a \mod p$.

Private key: a

Encryption: Bob chooses $r \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and computes $(u, v) = (g^r, Mh^r)$

Decryption: Given (u, v), Alice computes $M \equiv_p \frac{v}{u^a}$

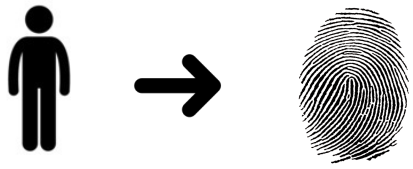
Justification: $\frac{v}{u^a} = \frac{Mh^r}{g^{ra}} \equiv_p M$

Remarque: re-usage of the same random r leads to a security flaw:

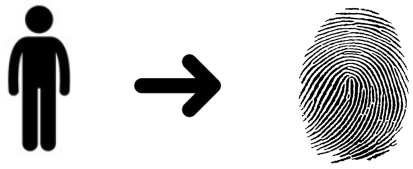
$$\frac{M_1 h^r}{M_2 h^r} \equiv_p \frac{M_1}{M_2}$$

Practical Inconvenience: Cipher is twice as long as plain text.

Hash Function (SHA-256, SHA-3)

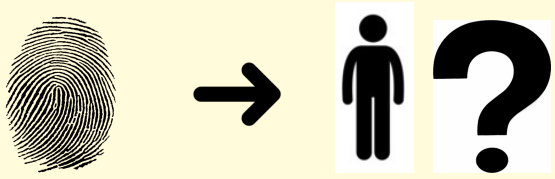


Hash Function (SHA-256, SHA-3)

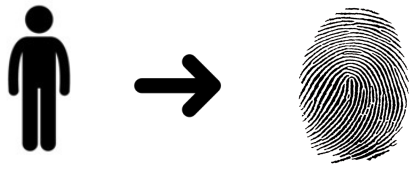


Security properties

- Pré-image Resistance

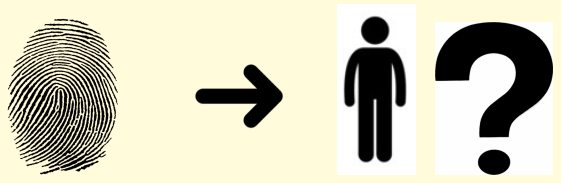


Hash Function (SHA-256, SHA-3)

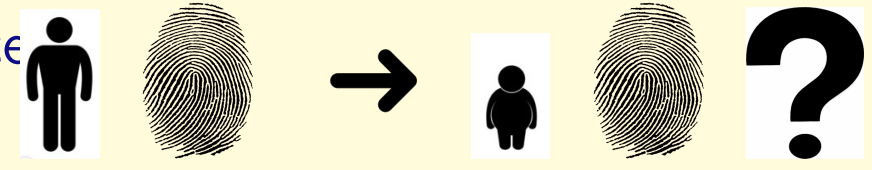


Security properties

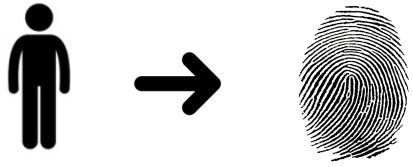
- Pré-image Resistance



- Second Pré-image Resistance

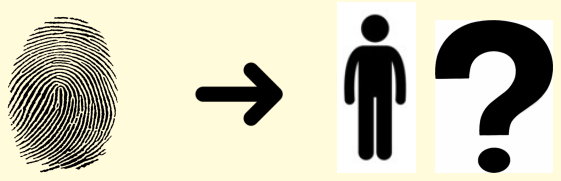


Hash Function (SHA-256, SHA-3)

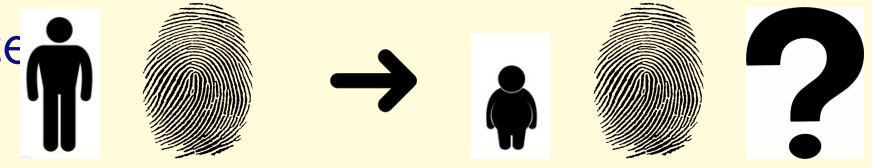


Security properties

- Pré-image Resistance



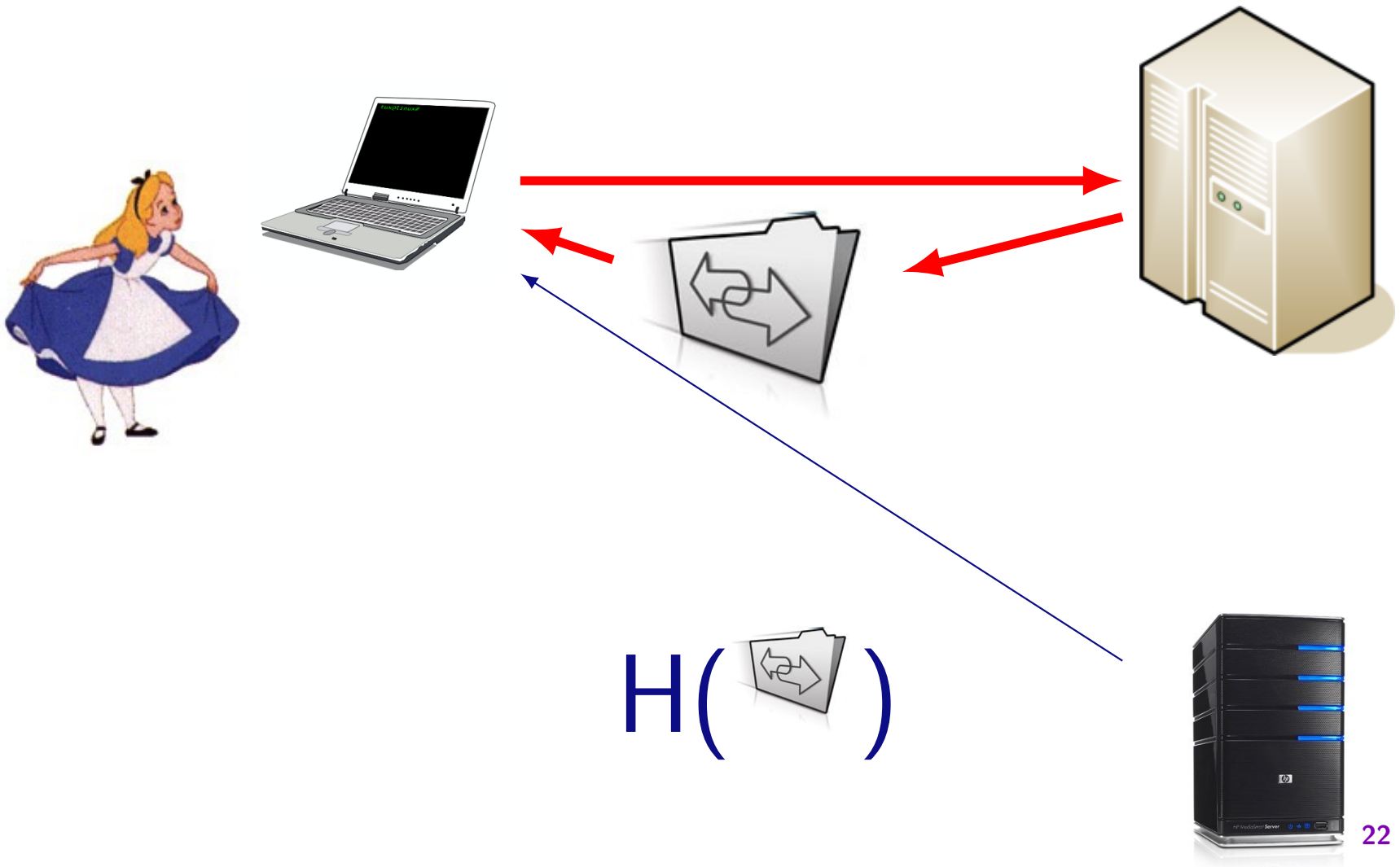
- Second Pré-image Resistance



- Collision Resistance

- Unkeyed Hash function: Integrity
- Keyed Hash function (Message Authentication Code): Authentification

Software Installation



MD5, MD4 and RIPEMD Broken

MD5(james.jpg)= e06723d4961a0a3f950e7786f3766338

MD5, MD4 and RIPEMD Broken

MD5(james.jpg)= e06723d4961a0a3f950e7786f3766338
MD5(barry.jpg) = e06723d4961a0a3f950e7786f3766338

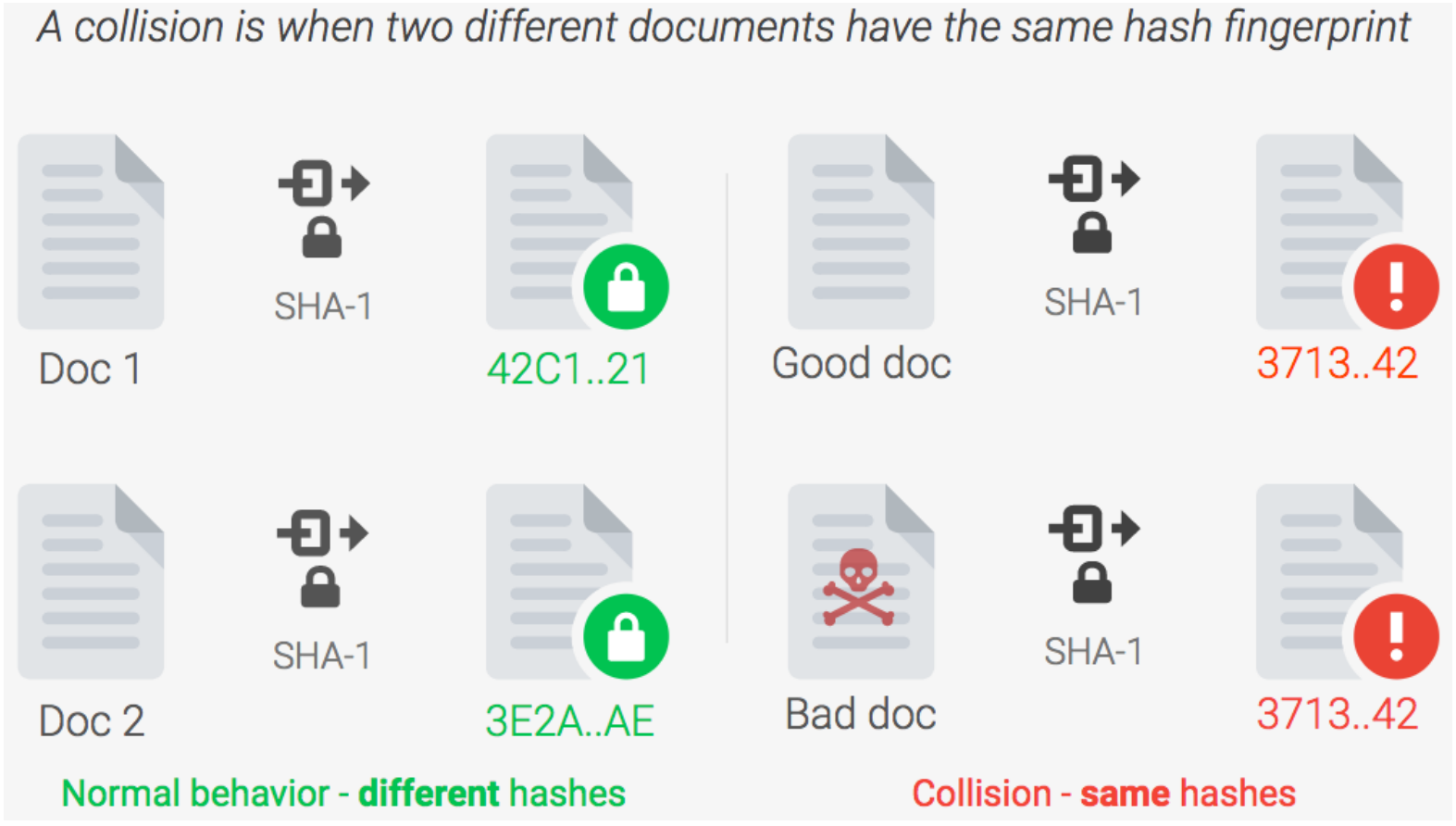
How to Break MD5 and Other Hash Functions, by Xiaoyun Wang, et al.

MD5 : Average run time on P4 1.6ghz PC: 45 minutes
MD4 and RIPEMD : Average runtime on P4 1.6ghz: 5 seconds

SHA-1 broken in 2017

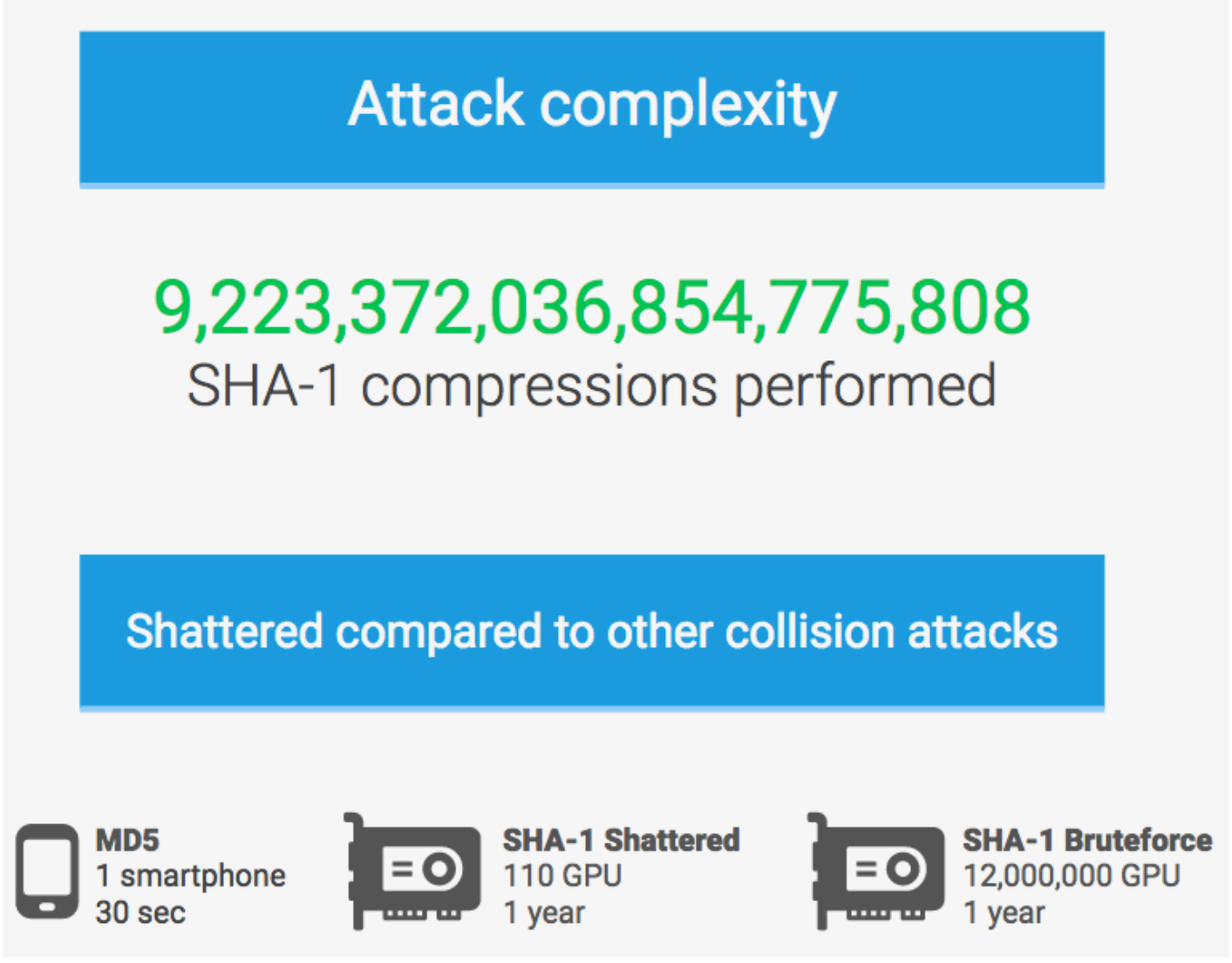
shattered.io

M. Stevens, P. Karpman, E. Bursztein, A. Albertini, Y. Markov



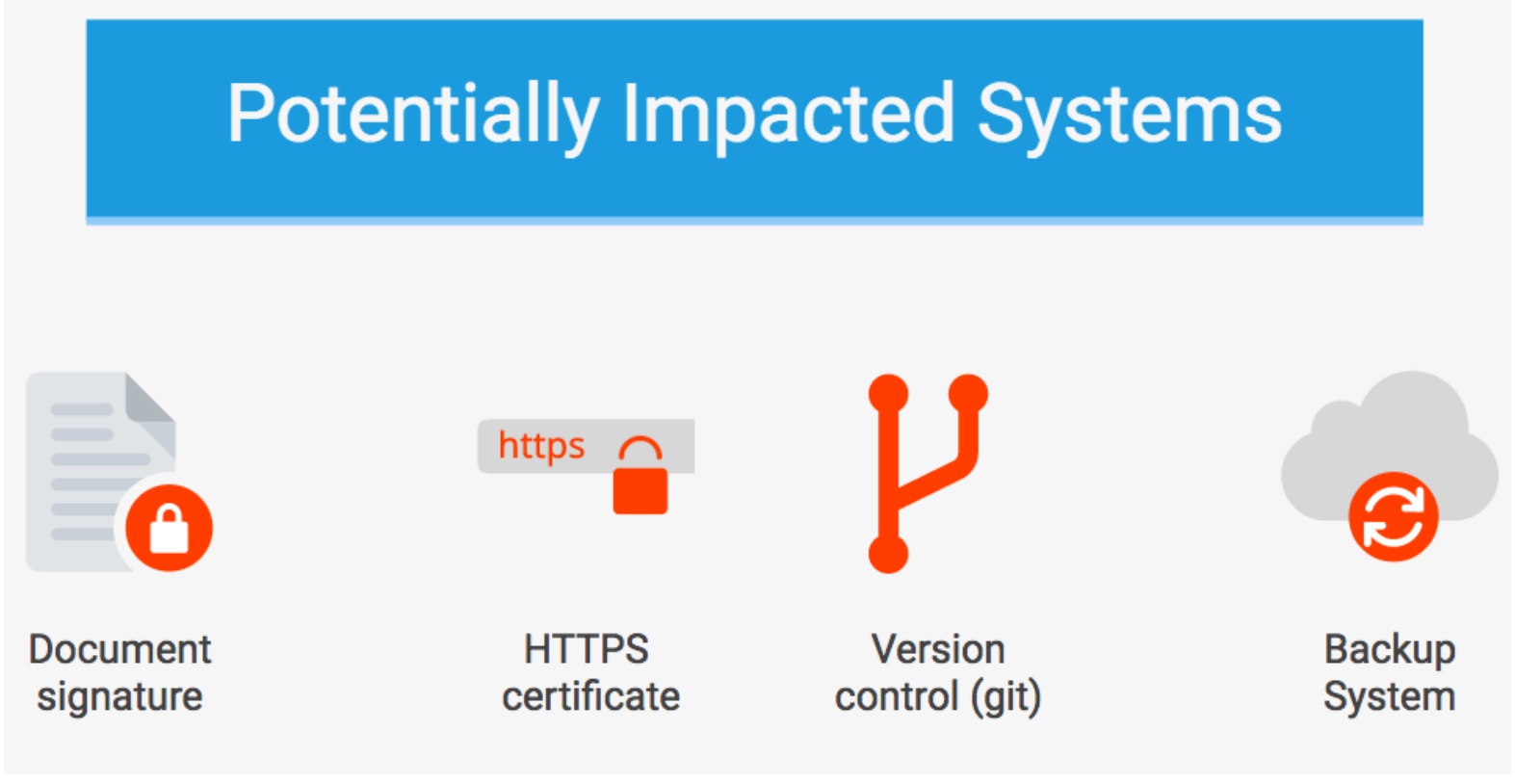
SHA-1 broken in 2017

shattered.io



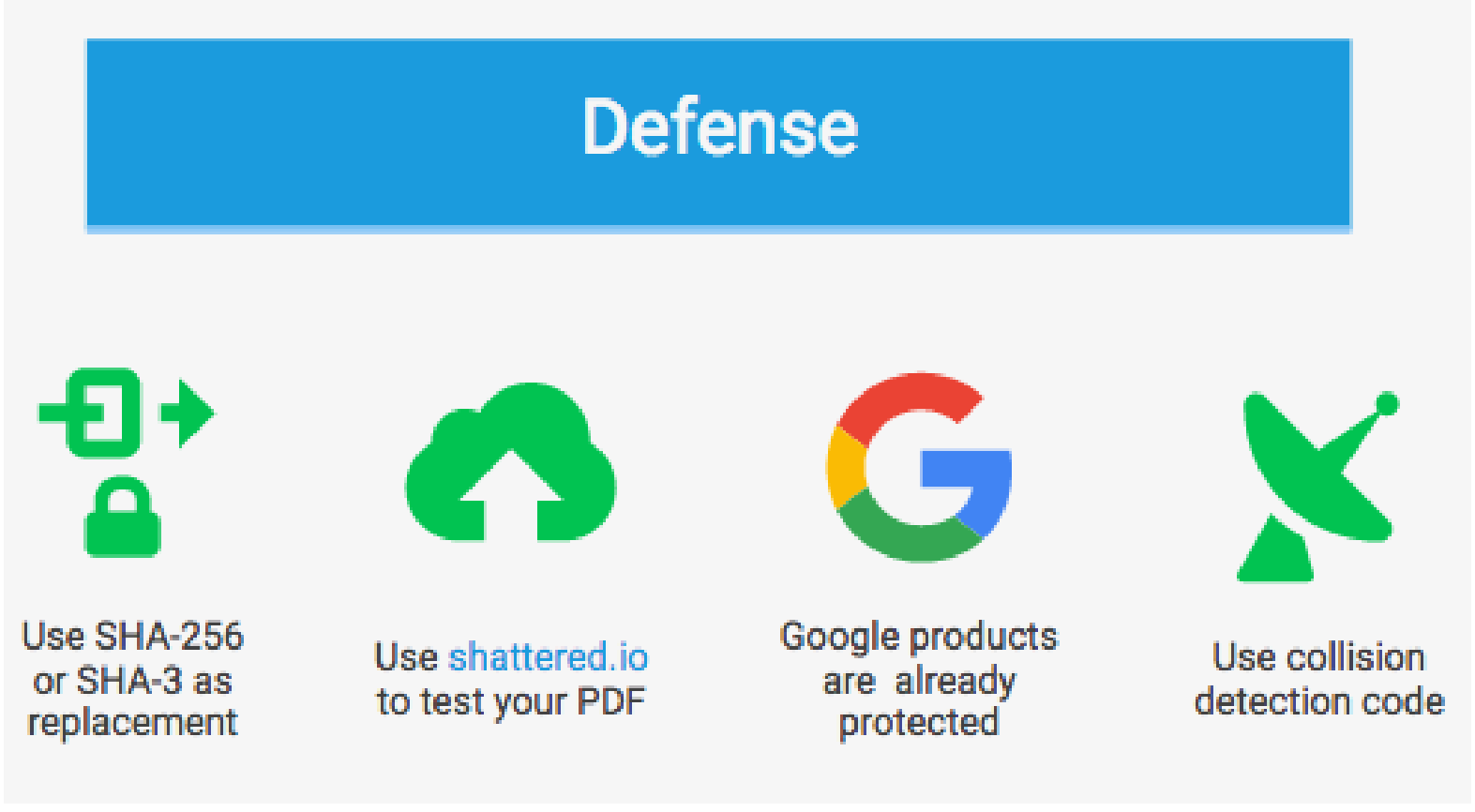
SHA-1 broken in 2017

shattered.io



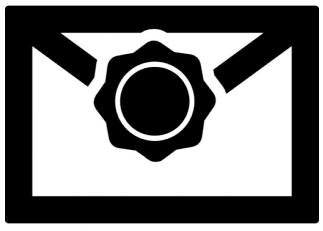
SHA-1 broken in 2017

shattered.io

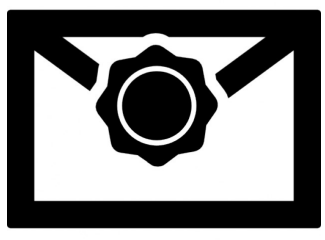


Signature

Signature



signature



verification

secret key

public key

RSA: $m^d \mod n$

Application : avoid to "*fraude au président*"

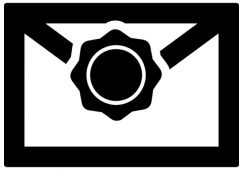
- In 2010 $>$ 485 billions of euros
- In 5 years 2.300 court cases

Application : avoid to "*fraude au président*"

- In 2010 $>$ 485 billions of euros
- In 5 years 2.300 court cases

Application : avoid to "*fraude au président*"

- In 2010 $>$ 485 billions of euros
- In 5 years 2.300 court cases

Solution : 

Broadcast encryption (Fiat-Noar 1994)

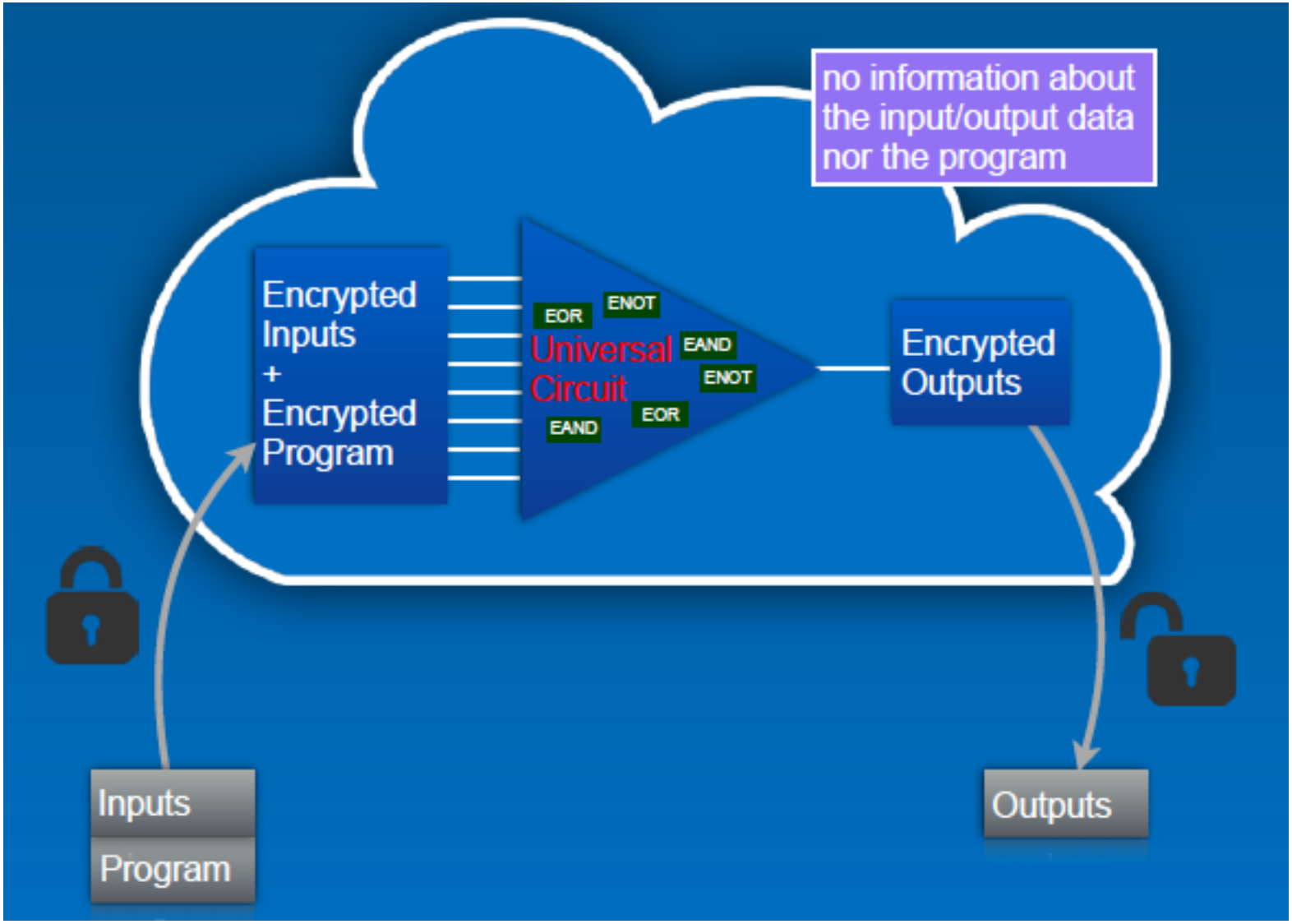
The sender can select the target group of receivers to control who access to the data like in PAYTV

Functional encryption [Boneh-Sahai-Waters 2011]

The user generates sub-keys K_y according to the input y to control the amount of shared data.
From $C = Encrypt(x)$, then $Decrypt(K_y, C)$, outputs $f(x, y)$

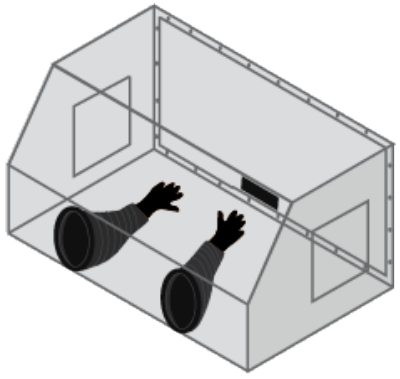
Outline

Fully Homomorphic Encryption [Gentry 2009]



Fully Homomorphic Encryption [Gentry 2009]

FHE: encrypt data, allow manipulation over data.
Symmetric Encryption (secret key) is enough



$$f(\{x_1\}_K, \{x_2\}_K, \ldots, \{x_n\}_K) = \{f(x_1, x_2, \ldots, x_n)\}_K$$

- Allows private storage
- Allows private computations
- Private queries in an encrypted database
- Private search: without leaking the content, queries and answers.

Rivest Adleman Dertouzos 1978

"Going beyond the storage/retrieval of encrypted data by permitting encrypted data to be operated on for interesting operations, in a public fashion?"

Partial Homomorphic Encryption

Definition (additively homomorphic)

$$E(m_1) \otimes E(m_2) \equiv E(m_1 \oplus m_2).$$

Applications

- Electronic voting
- Secure Fonction Evaluation
- Private Multi-Party Trust Computation
- Private Information Retrieval
- Private Searching
- Outsourcing of Computations (e.g., Secure Cloud Computing)
- Private Smart Metering and Smart Billing
- Privacy-Preserving Face Recognition
- ...

Brief history of partially homomorphic cryptosystems

$$Enc(a,k) * Enc(b,k) = Enc(a * b, k)$$

Year	Name	Security hypothesis	Expansion
1977	RSA	factorization	
1982	Goldwasser - Micali	quadratic residuosity	$\log_2(n)$
1994	Benaloh	higher residuosity	> 2
1998	Naccache - Stern	higher residuosity	> 2
1998	Okamoto - Uchiyama	p-subgroup	3
1999	Paillier	composite residuosity	2
2001	Damgaard - Jurik	composite residuosity	$\frac{d+1}{d}$
2005	Boneh - Goh - Nissim	ECC Log	
2010	Aguilar-Gaborit-Herranz	SIVP integer lattices	

Expansion factor is the ration ciphertext over plaintext.

Scheme Unpadded RSA

If the RSA public key is modulus m and exponent e, then the encryption of a message x is given by

$$\mathcal{E}(x) = x^e \mod m$$

$$\begin{aligned} \mathcal{E}(x_1) \cdot \mathcal{E}(x_2) &= x_1^e x_2^e \mod m \\ &= (x_1 x_2)^e \mod m \\ &= \mathcal{E}(x_1 \cdot x_2) \end{aligned}$$

Scheme ElGamal

In the ElGamal cryptosystem, in a cyclic group G of order q with generator g, if the public key is (G, q, g, h), where $h = g^x$ and x is the secret key, then the encryption of a message m is $\mathcal{E}(m) = (g^r, m \cdot h^r)$, for some random $r \in \{0, \ldots, q-1\}$.

$$\begin{aligned} \mathcal{E}(m_1) \cdot \mathcal{E}(m_2) &= (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) \\ &= (g^{r_1+r_2}, (m_1 \cdot m_2) h^{r_1+r_2}) \\ &= \mathcal{E}(m_1 \cdot m_2) \end{aligned}$$

Fully Homomorphic Encryption

$$Enc(a,k) * Enc(b,k) = Enc(a * b, k)$$
$$Enc(a,k) + Enc(b,k) = Enc(a + b, k)$$
$$f(Enc(a,k), Enc(b,k)) = Enc(f(a,b), k)$$

Fully Homomorphic encryption

- Craig Gentry (STOC 2009) using lattices
- Marten van Dijk; Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan using integer
- Craig Gentry; Shai Halevi. "A Working Implementation of Fully Homomorphic Encryption"
- ...

Simple SHE: SGHV Scheme [vDGHV10]

Public error-free element : $x_0 = q_0 \cdot p$
Secret key $sk = p$

Encryption of $m \in \{0, 1\}$

$$c = q \cdot p + 2 \cdot r + m$$

where q is a large random and r a small random.

Simple SHE: SGHV Scheme [vDGHV10]

Public error-free element : $x_0 = q_0 \cdot p$
Secret key $sk = p$

Encryption of $m \in \{0, 1\}$

$$c = q \cdot p + 2 \cdot r + m$$

where q is a large random and r a small random.

Decryption of c

$$m = (c \mod p) \mod 2$$

Outline

Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

Example: e-voting

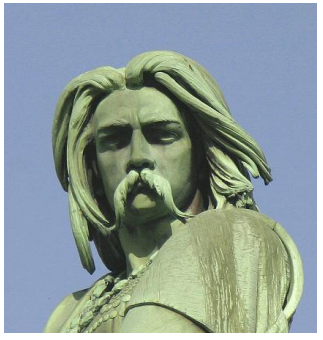
- An e-voting system should ensure that
  - only registered voters vote,
  - each voter can only vote once,
  - integrity of votes,
  - privacy of voting information (only used for tallying), and
  - availability of system during voting period

Outline

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something
without revealing any information

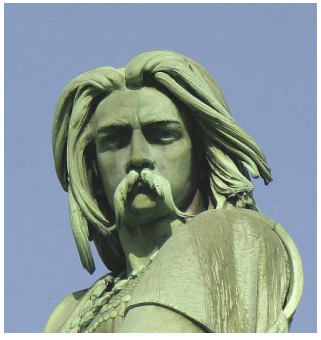


Verifier (V)

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something
without revealing any information

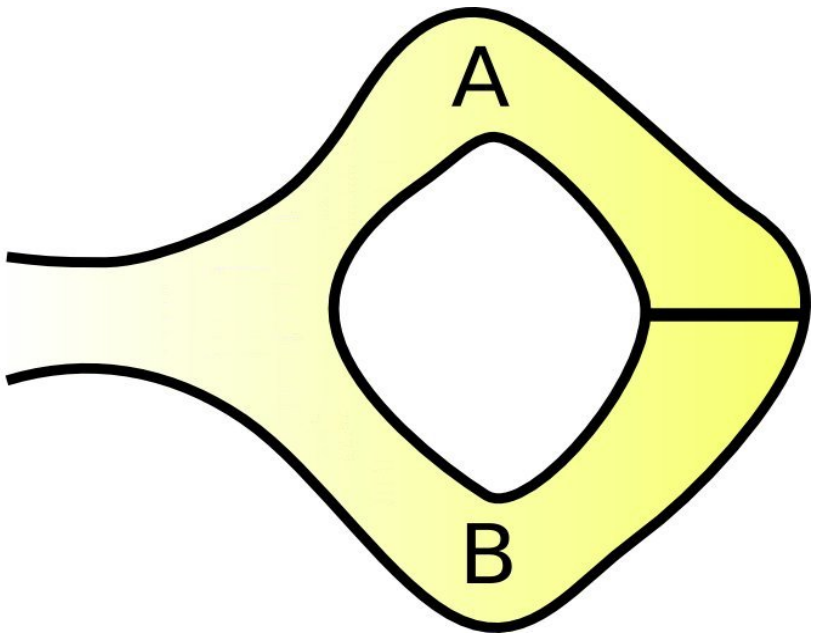


Verifier (V)

Applications:

- Authentication systems: prove its identity to someone using a password without reavealing anything about the secret.
- Prove that a praticipant behavior is correct according to the protocol (e.g. integrity of ballots in vote).
- Group signature, secure multiparty computation, e-cash ...

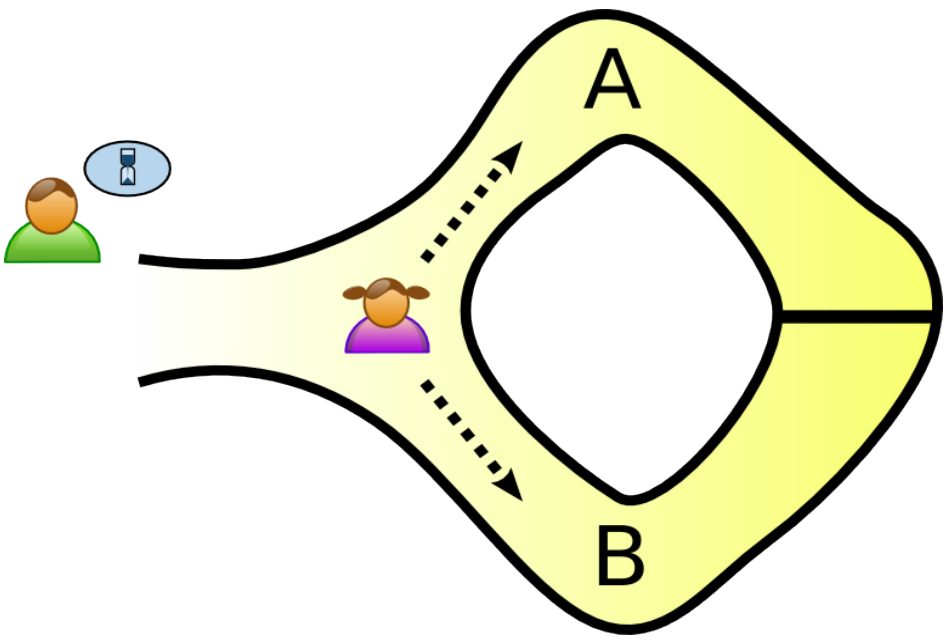
Cave example (0)



Door with a secret code

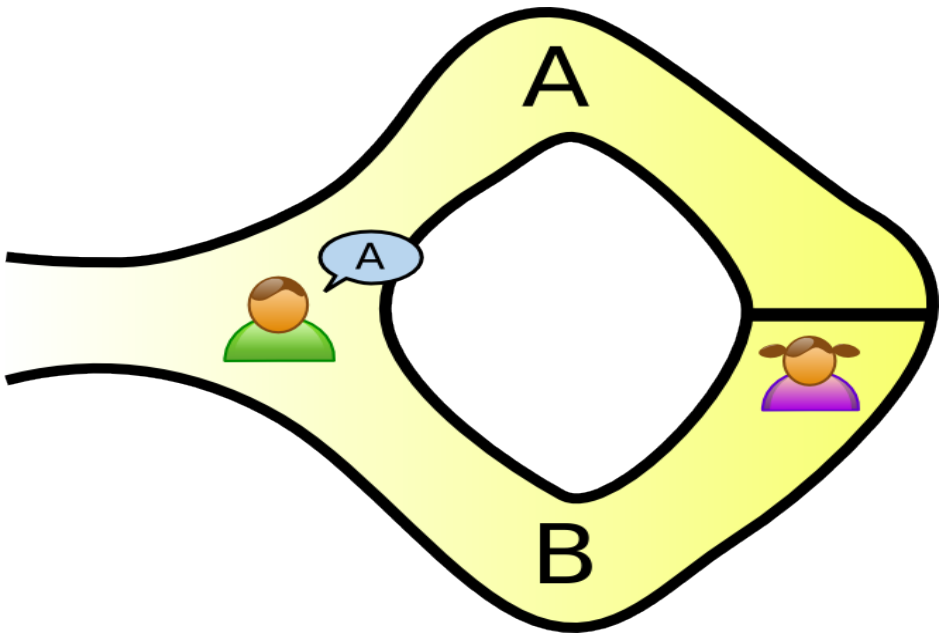
Cave example (I)

V waits outside while P chooses a path



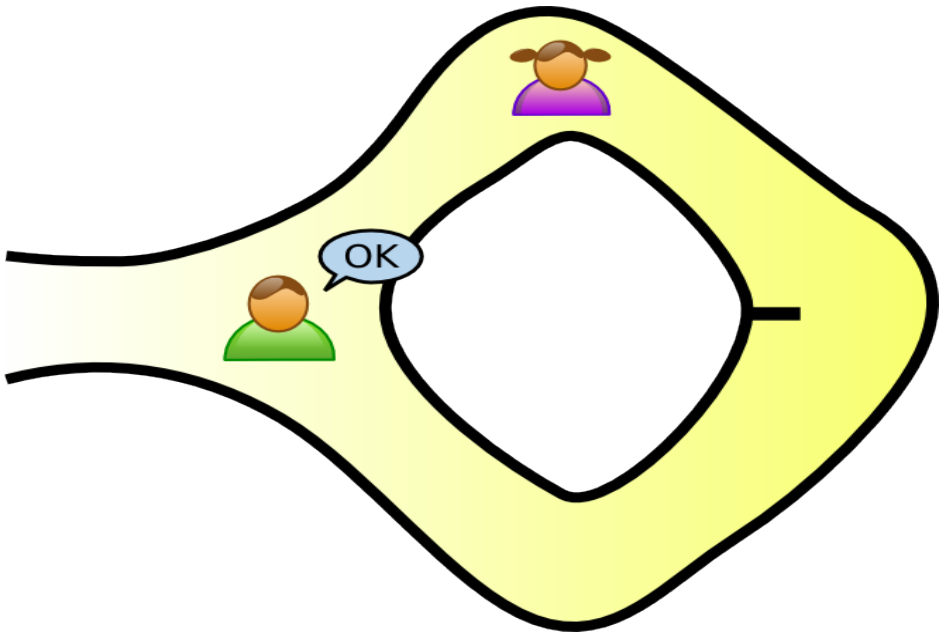
Cave example (II)

V enters and shouts the name of a path



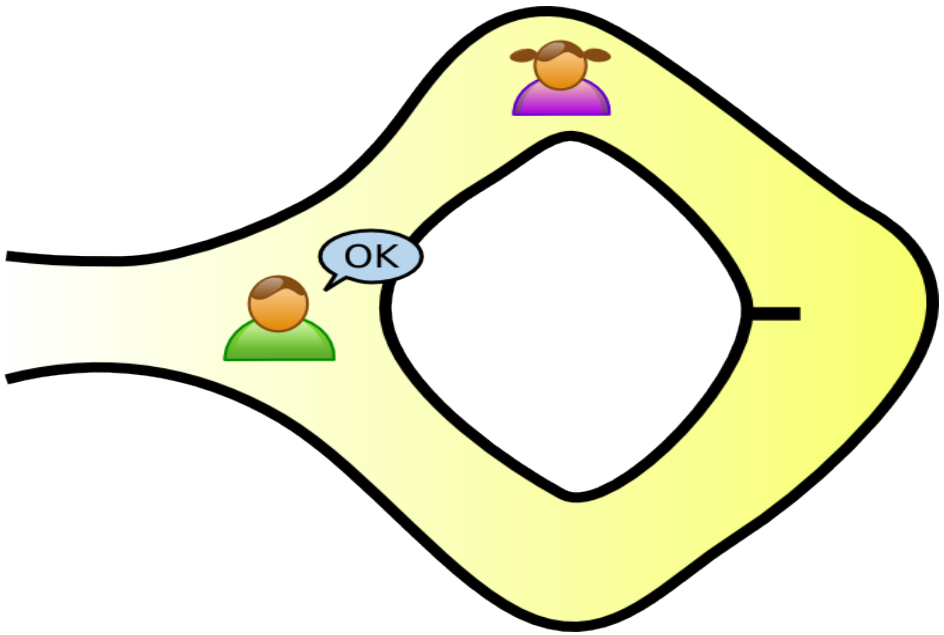
Cave example (III)

P returns along the desired path (using the secret if necessary)



Cave example (III)

P returns along the desired path (using the secret if necessary)

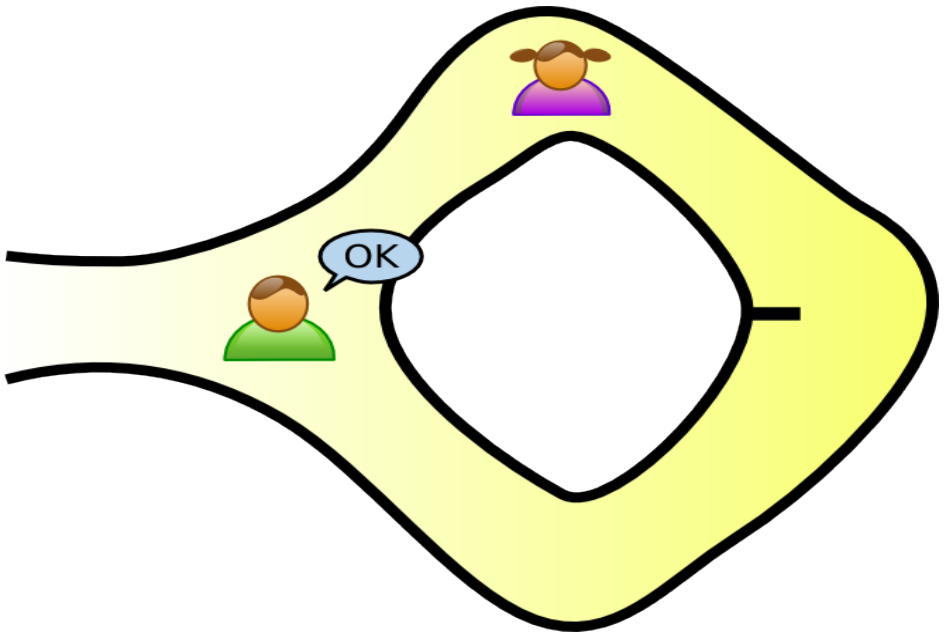


$A =$ "P does not know the secret"
is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

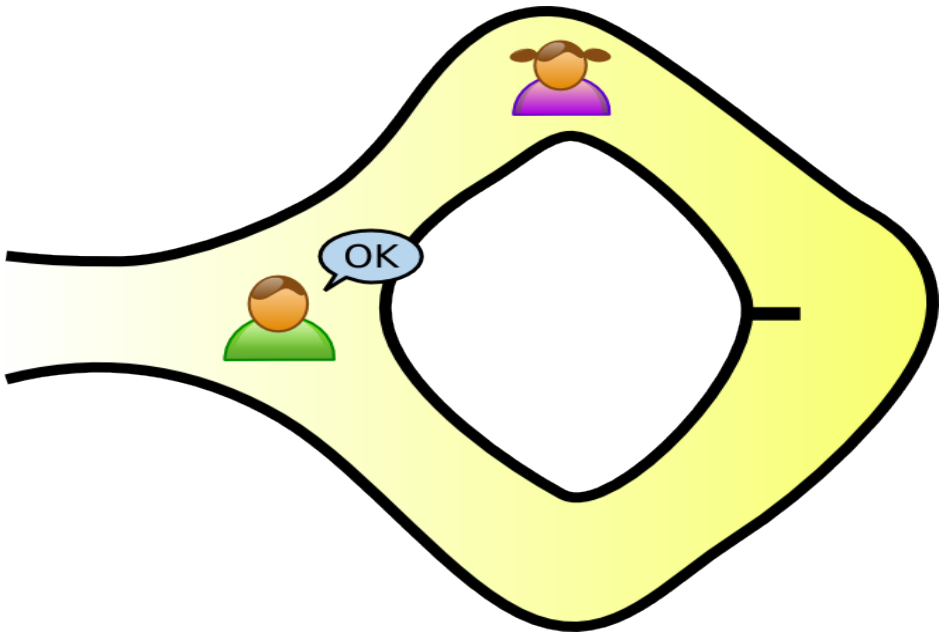
$$Pr[A] = \frac{1}{2}$$

After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

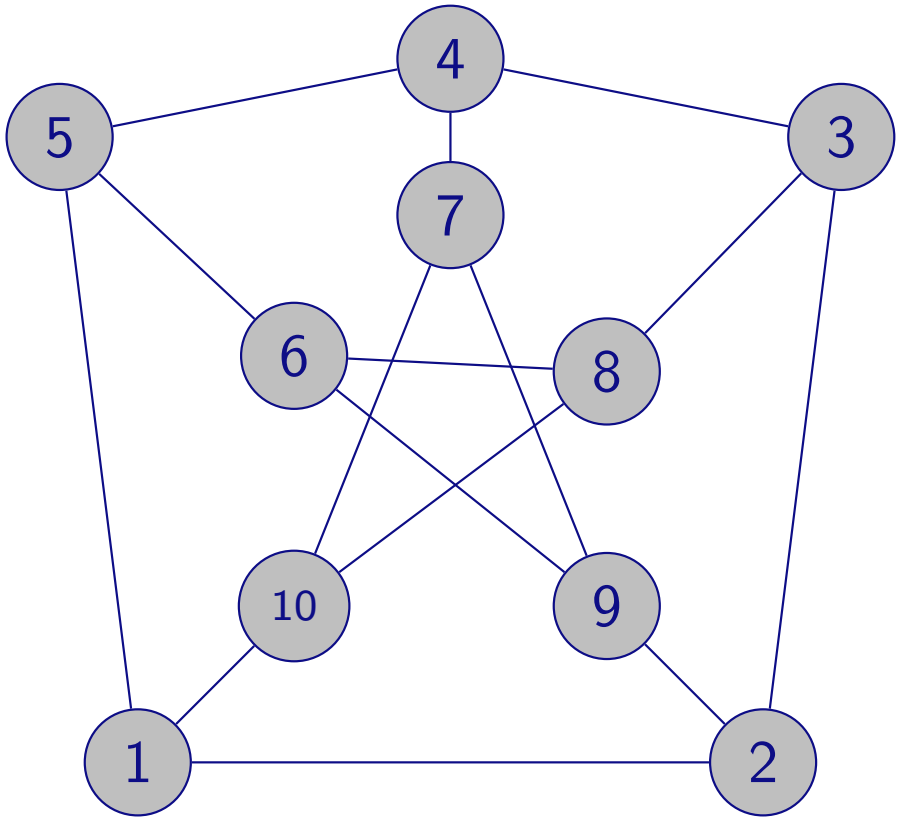
After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

$\overline{A} =$ "P knows the secret", then

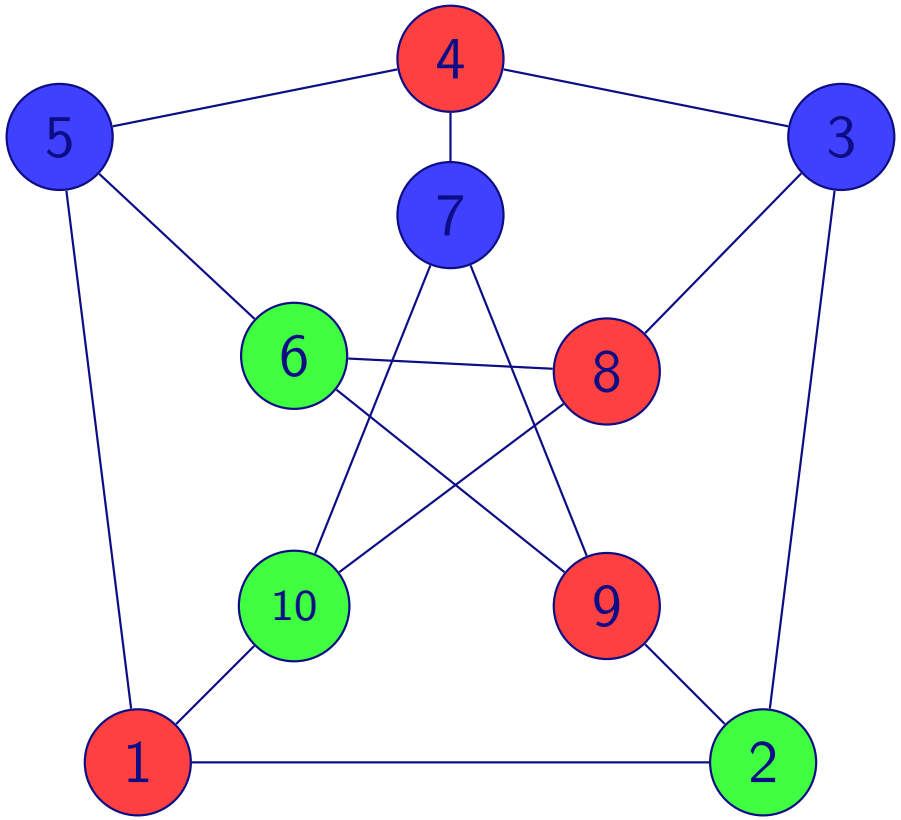
$$Pr[\overline{A}] = 1 - Pr[A] = 1 - (\frac{1}{2})^k$$

Graph 3-coloring is NP-complete: ● ● ●



Petersen graph

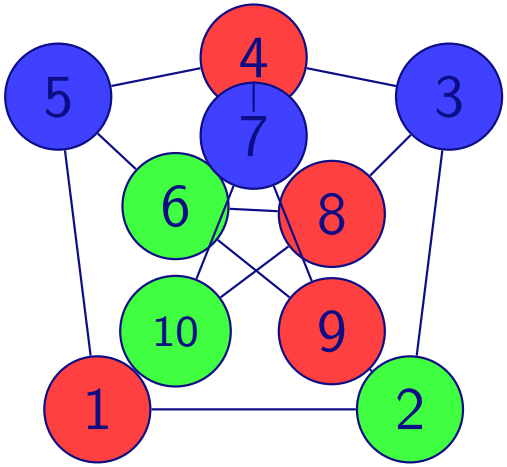
Graph 3-coloring is NP-complete: ● ● ●

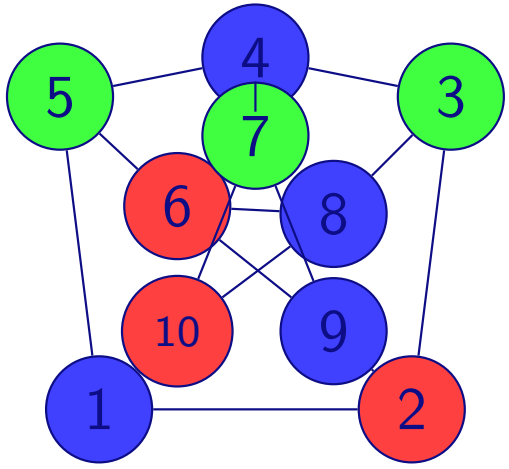


Petersen graph

P wants to prove to V his 3-coloring of $G = (E, V)$

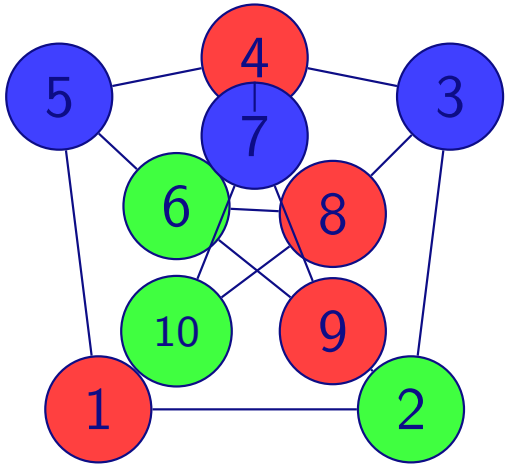
P selects a permutation π of the 3 colors.

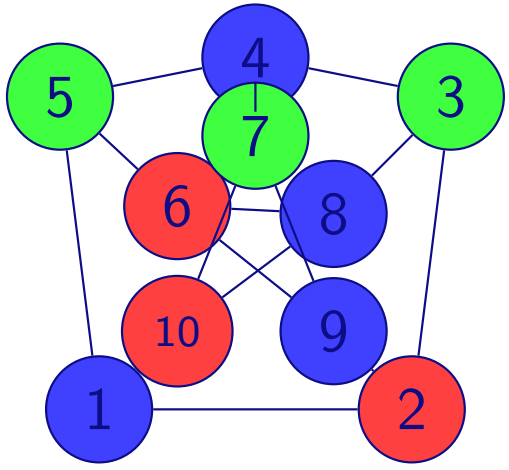
$\pi($ 

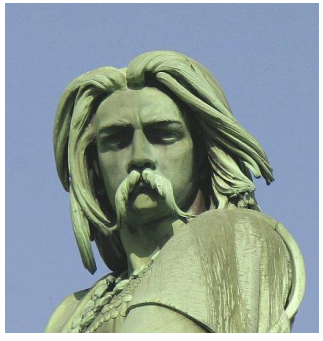
$)=$ 

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

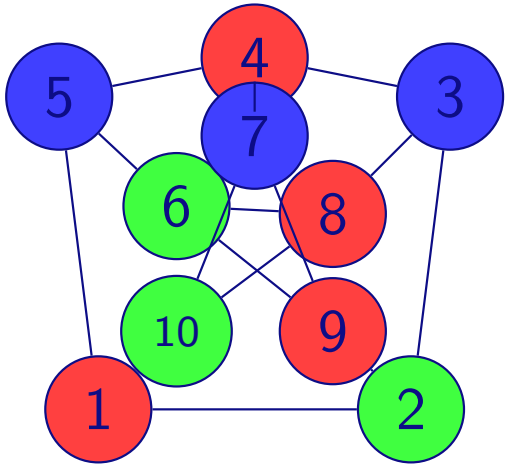
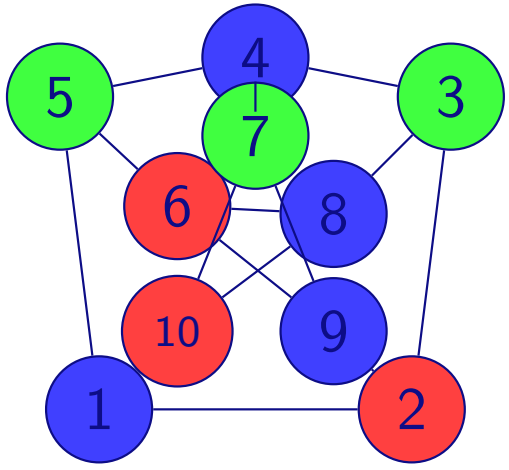
$)=$ 



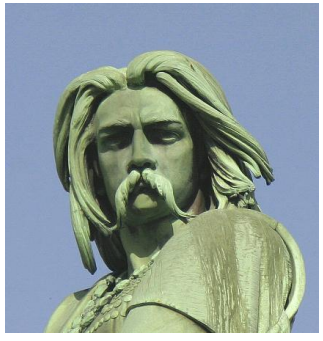
Chooses $\forall u \in V, r_u$

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($  $)=$ 

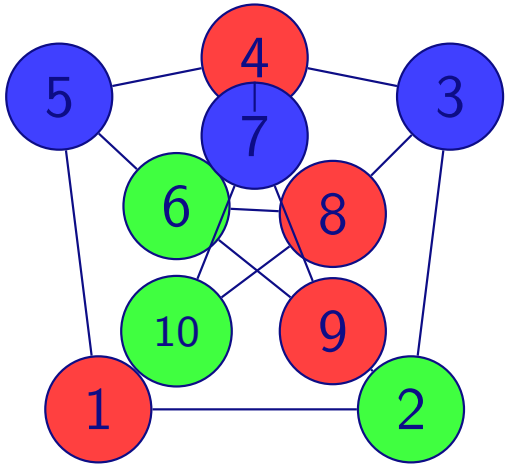
$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

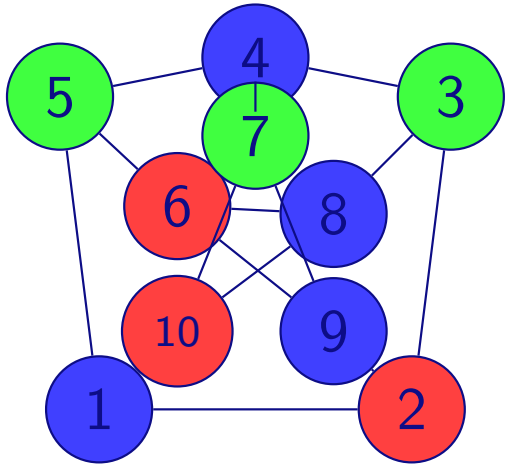


Chooses $\forall u \in V, r_u$

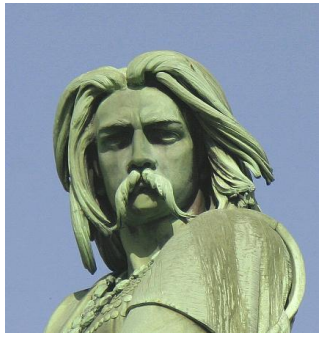
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

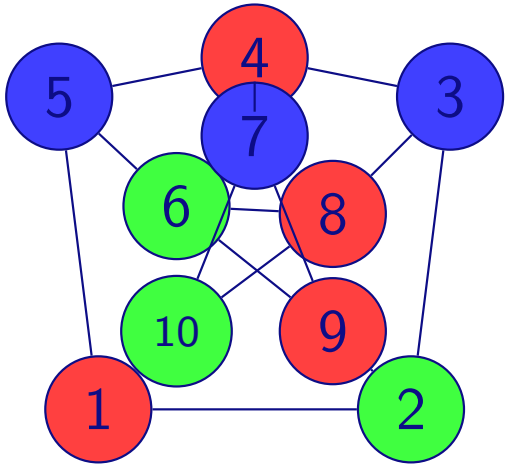


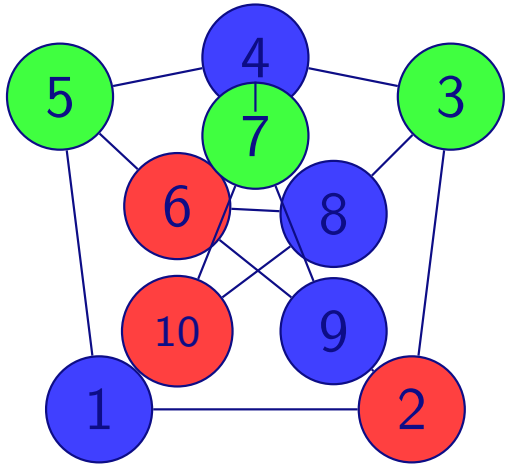
Chooses $\forall u \in V, r_u$

Chooses i and j

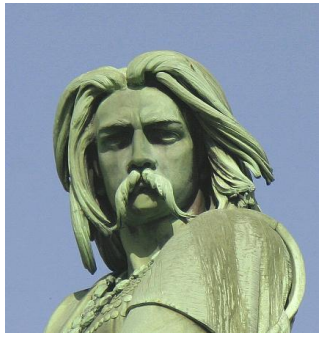
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$

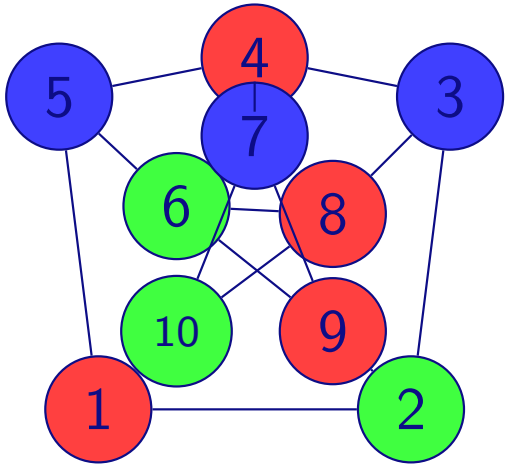


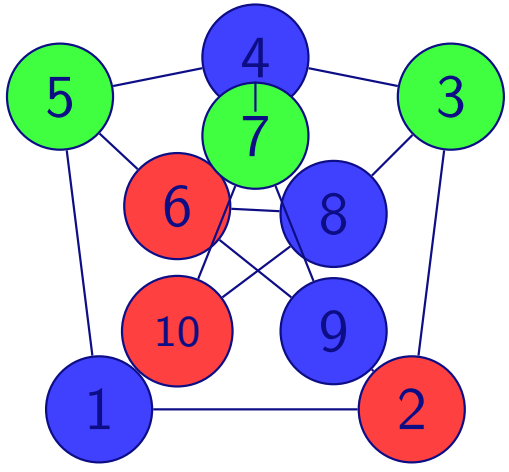
Chooses $\forall u \in V, r_u$

Chooses i and j

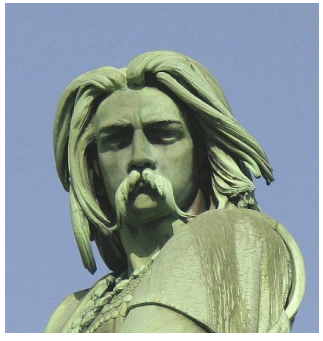
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\leftarrow\!\!\!\!- \; u_i, u_j \; \leftarrow\!\!\!\!-$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

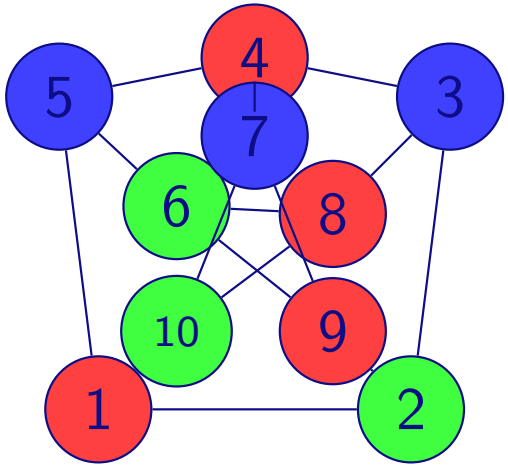


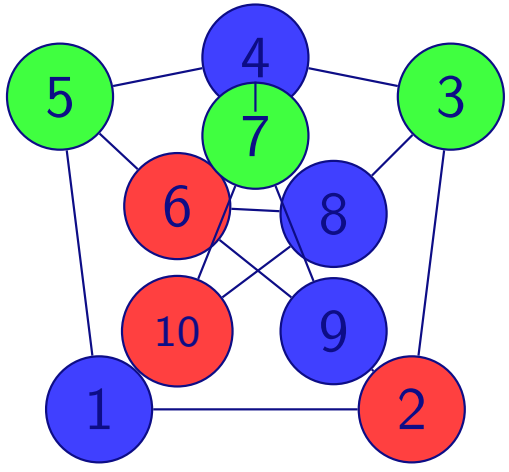
Chooses $\forall u \in V, r_u$

Chooses i and j

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

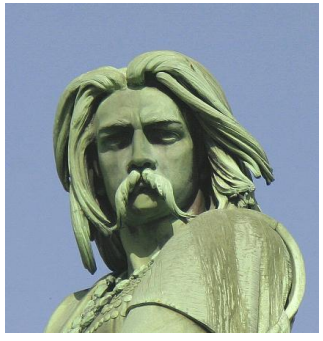
$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

V accepts, if $e_{u_i} = H(\pi(c(u_i))||r_{u_i})$ and $e_{u_j} = H(\pi(c(u_j))||r_{u_j})$



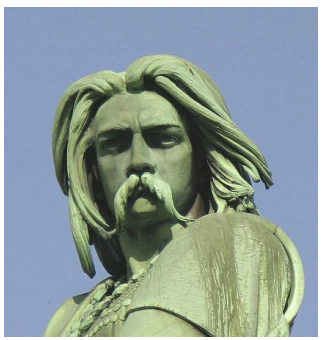
Chooses i and j

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

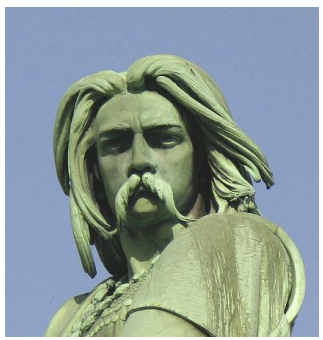


Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$



Chooses a random r

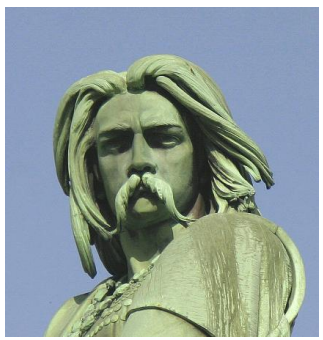
Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

$\longrightarrow t = g^r \longrightarrow$



Chooses a random r

Schnorr Protocol, 1991

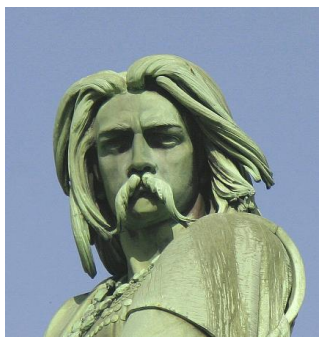
Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

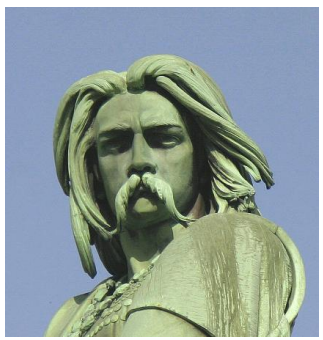
Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

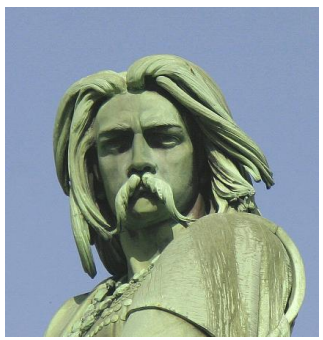
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

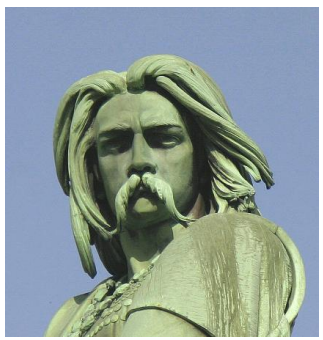
Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$

V accepts, if $t \cdot y^c = g^s$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

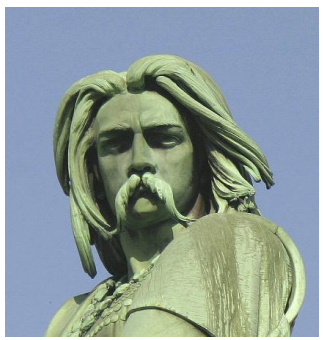
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

V accepts, if $t \cdot y^c = g^s$

$$t \cdot y^c = g^r \cdot (g^x)^c = g^{r+x \cdot c} = g^s$$

Outline

Today

1. Historic of Cryprography
2. Cryptographic primitives
3. Properties security

Ron Rivest

"Once you have something on the Internet, you are telling the world, please come hack me."