CS547A
Cryptography and Data Security

Lecture 02

Claude Crépeau

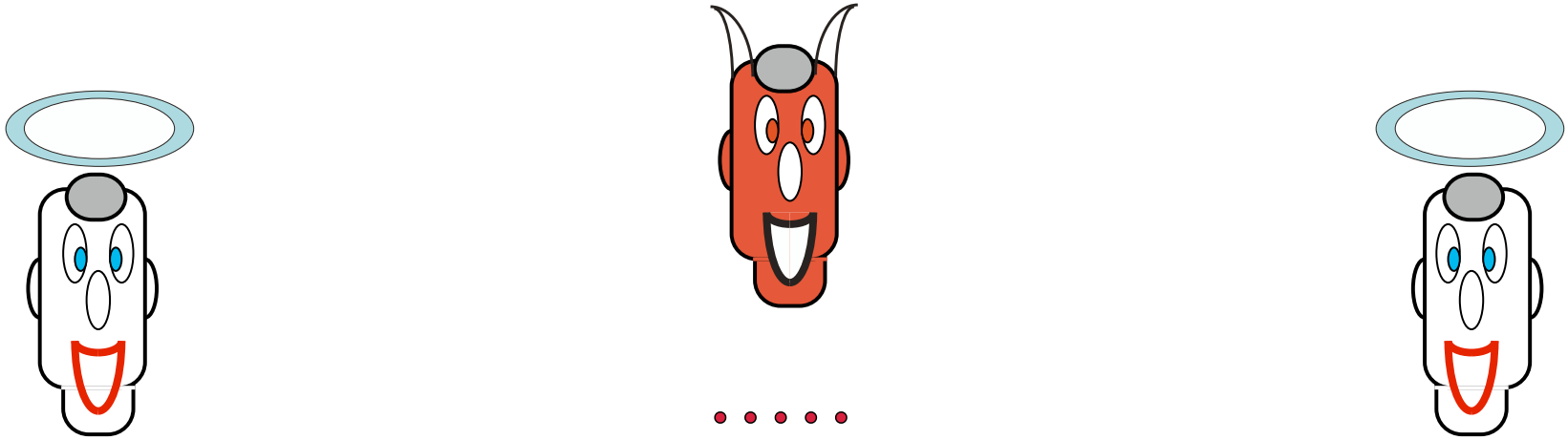
School of Computer Science
McGill University

Complexity

Theoretical

Cryptography

Complexity Theoretical Symmetric Cryptography



. . . . .

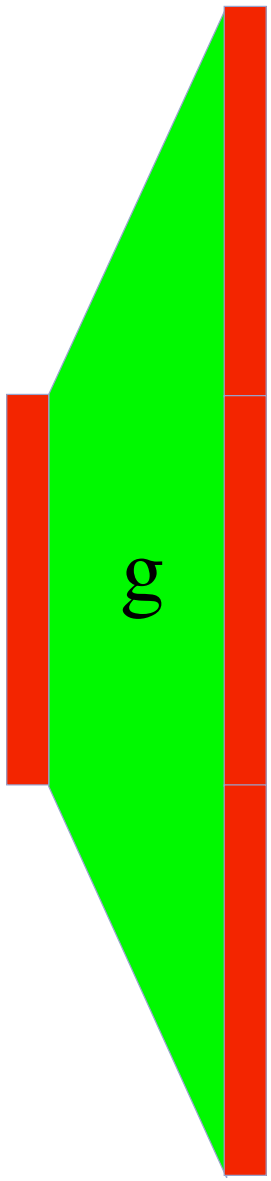
encryption

authentication

identification

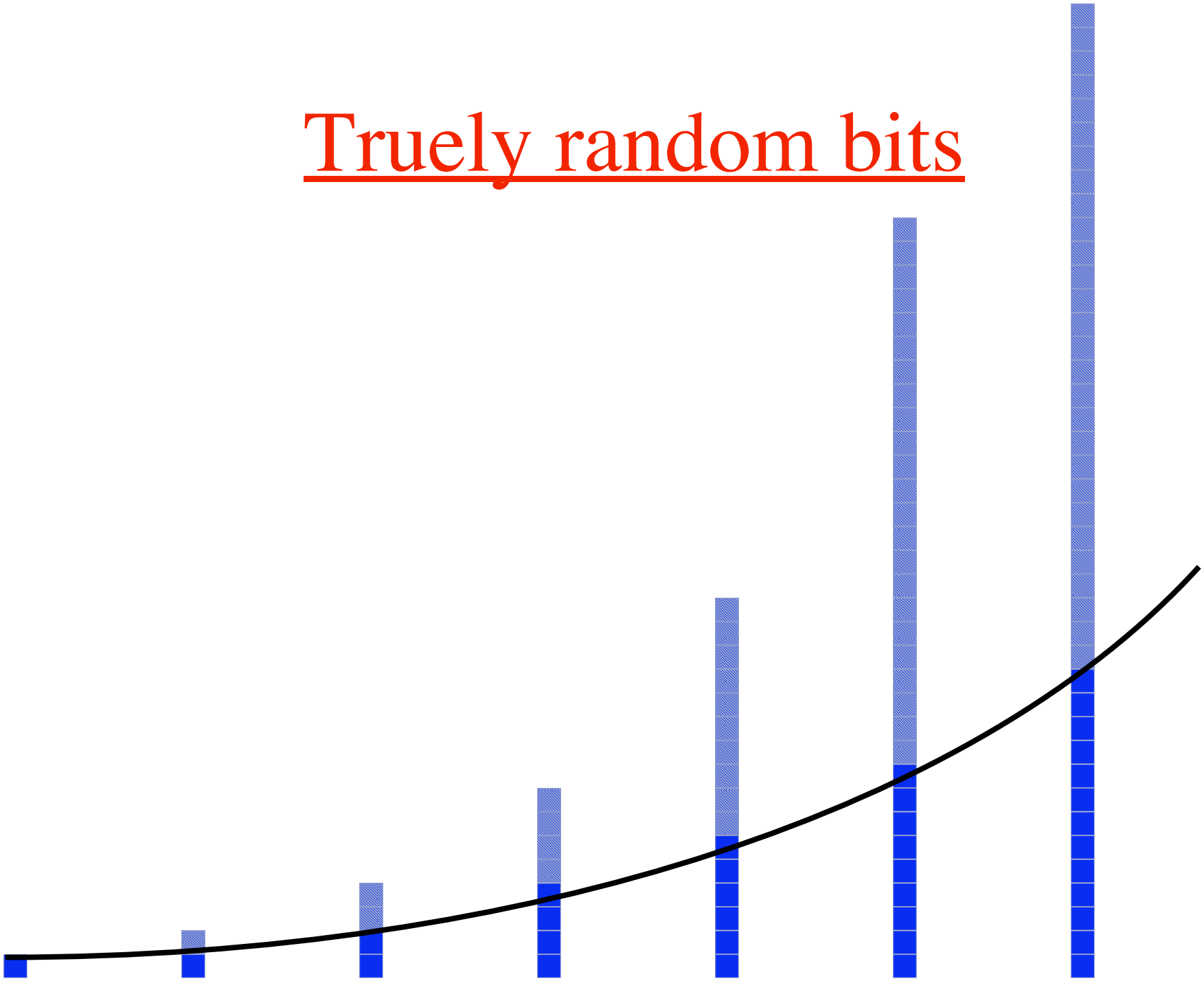
. . . . .

pseudo-random bit generator

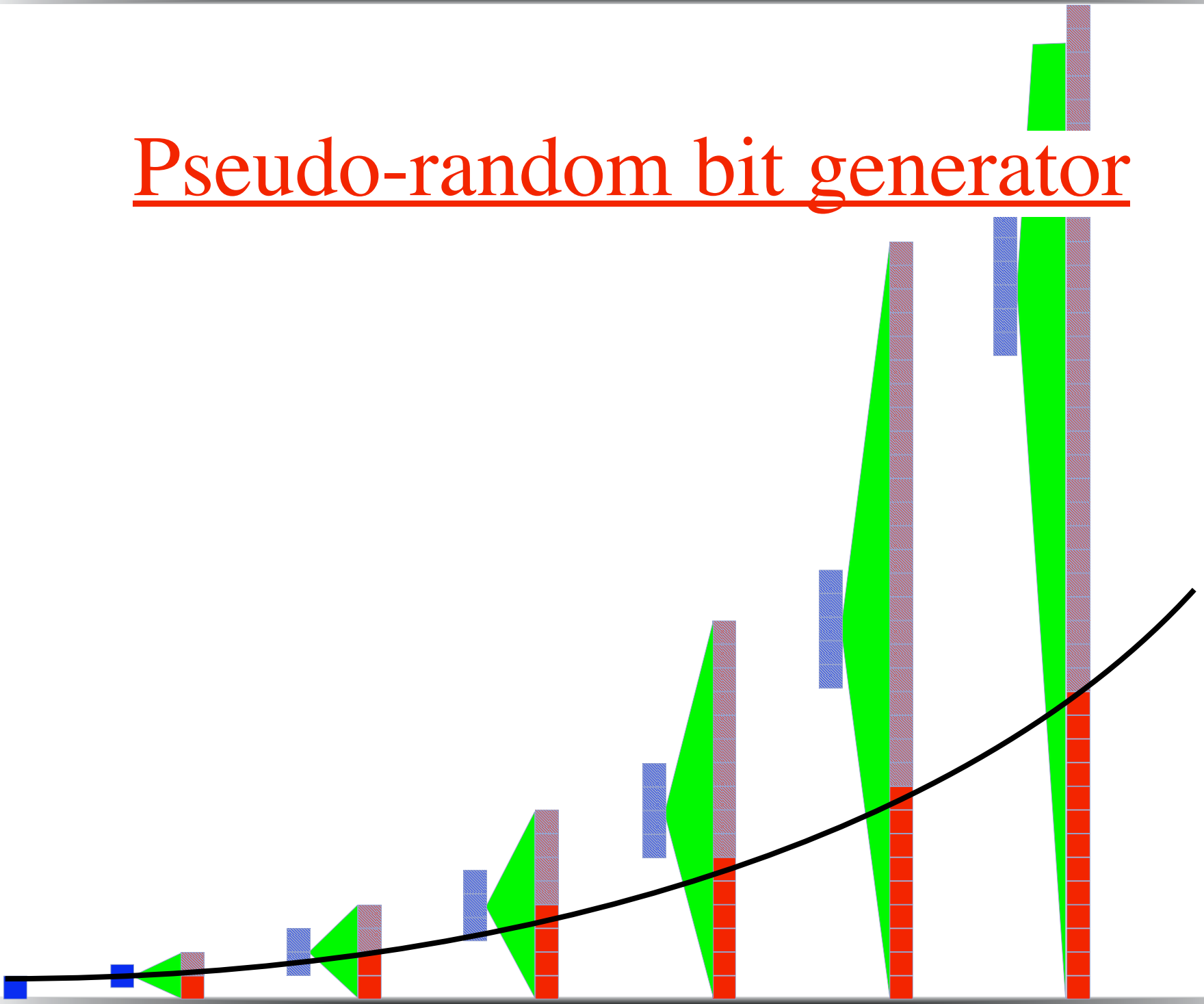
RANDOM x 

g(x) SEEMS RANDOM

Truely random bits

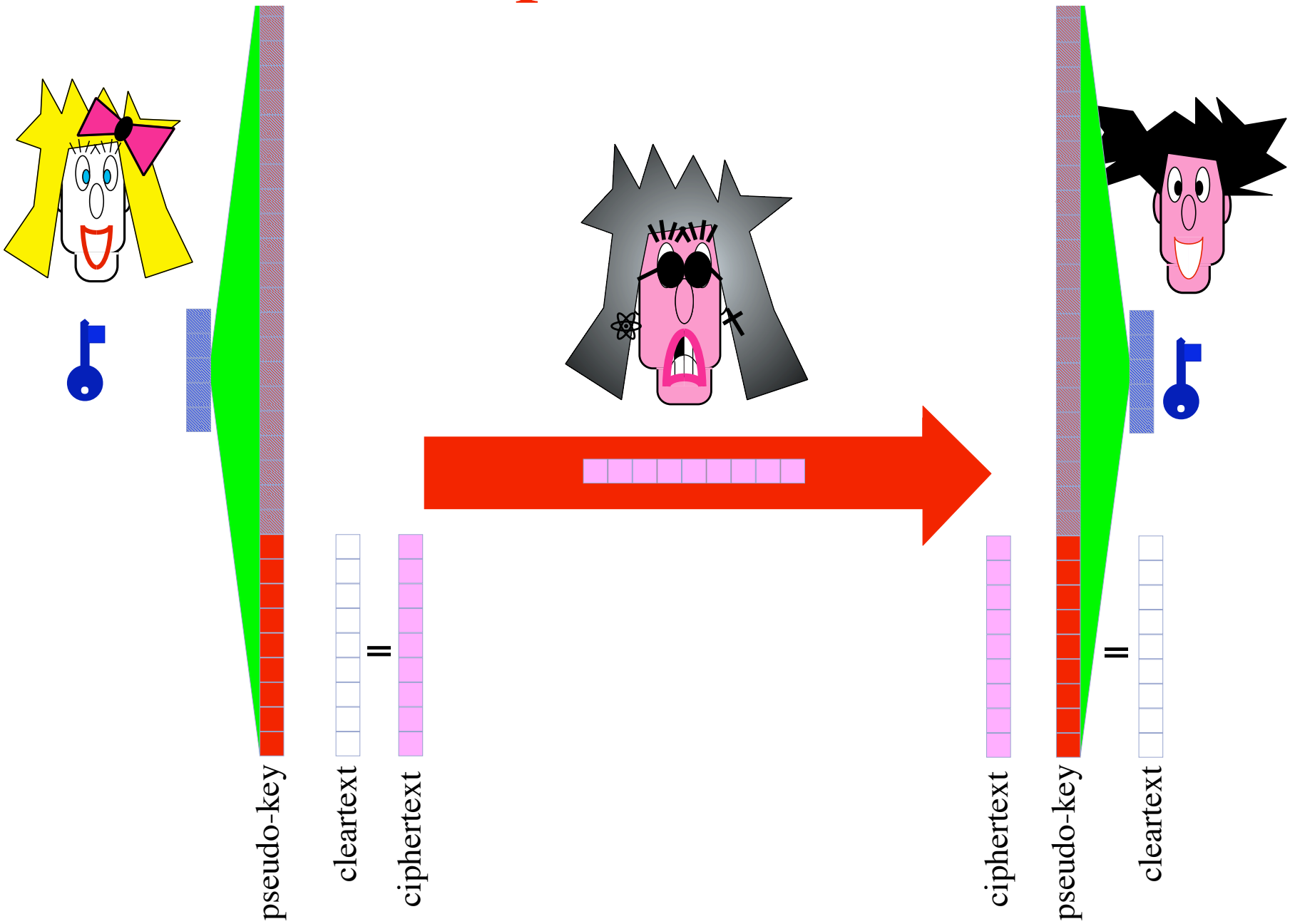


Pseudo-random bit generator

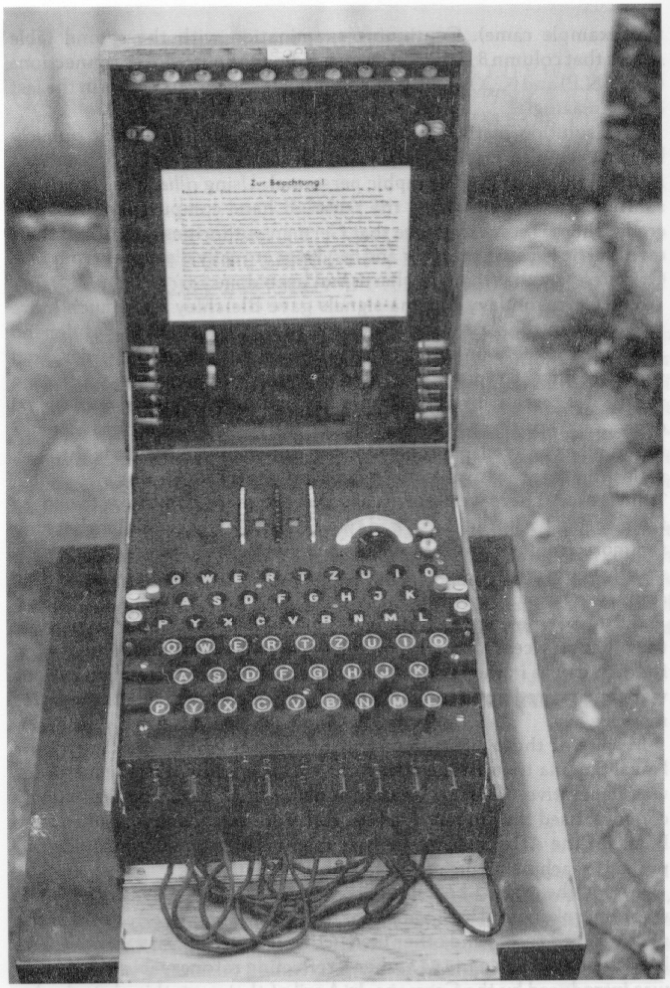


encryption

Stream-cipher from PRBG

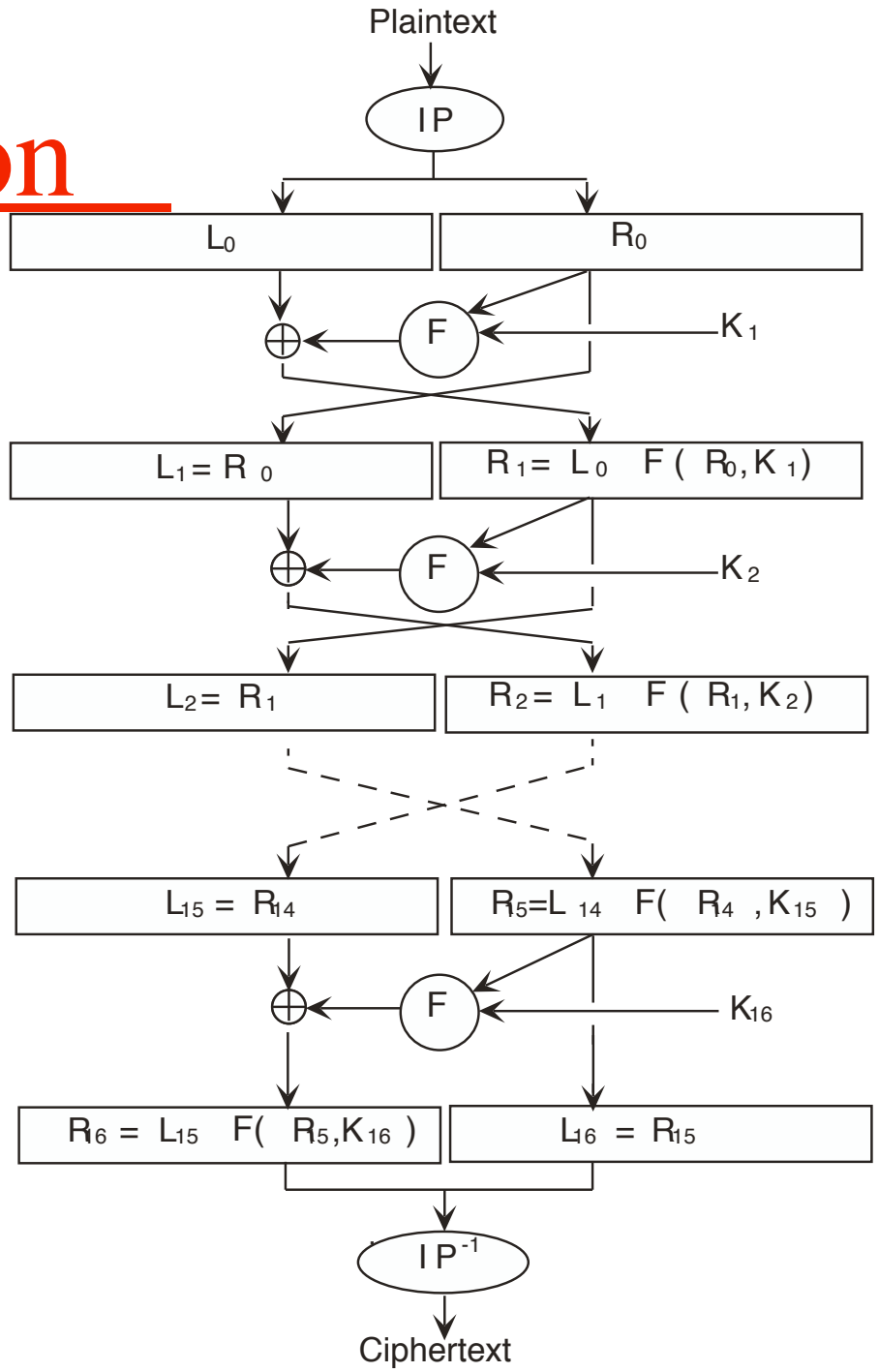


ENIGMA



GERMAN ARMY MILITARY ENIGMA. THIS MODEL WAS THE MOST WIDELY USED VERSION OF THE GERMAN WAR-TIME ENIGMAS.

Data Encryption Standard



Advanced Encryption Standard

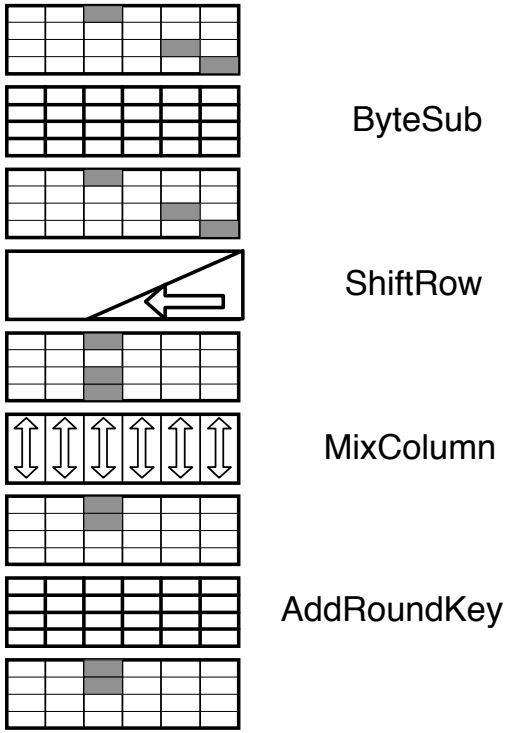
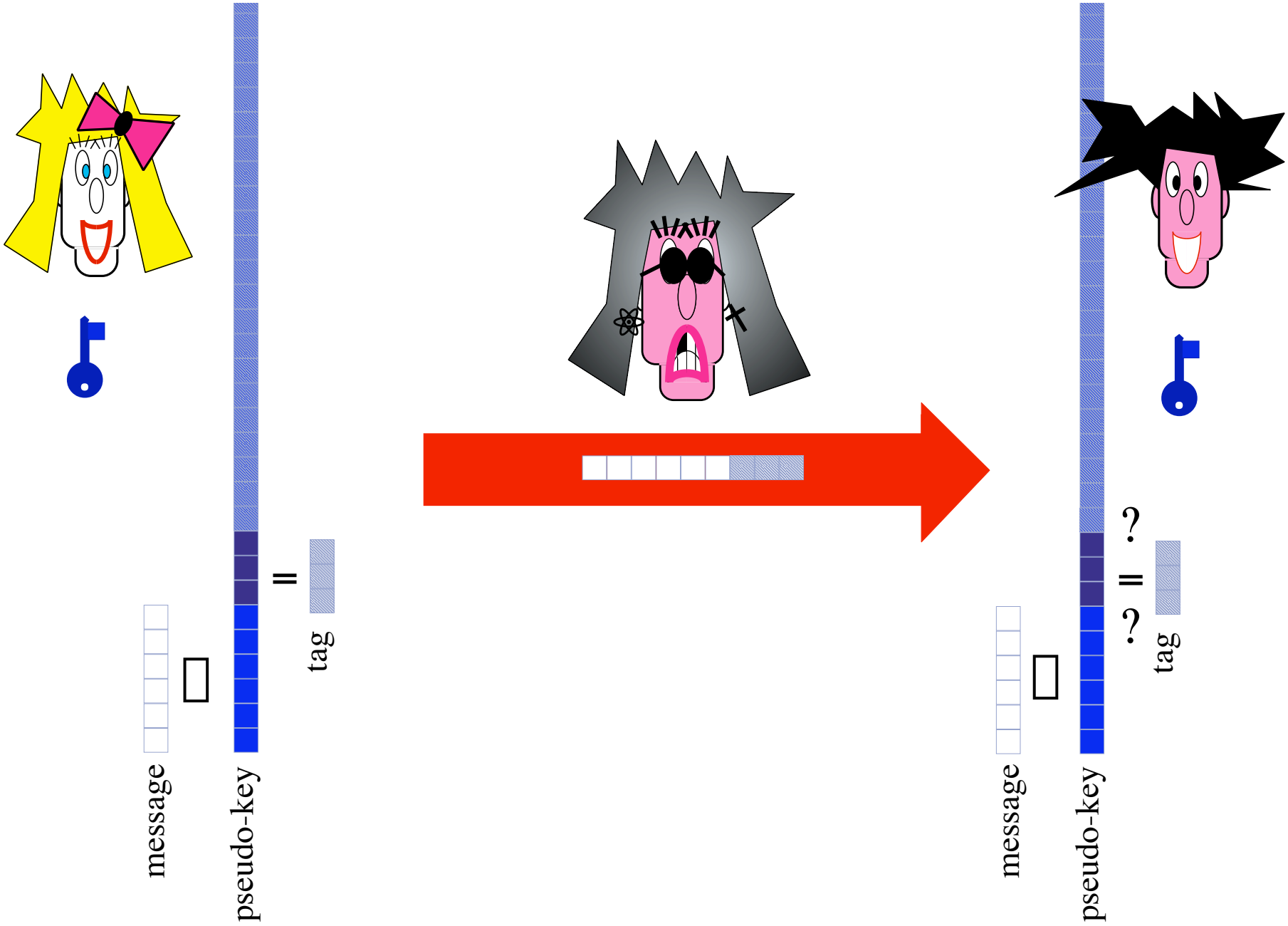


Figure 7: Propagation of activity pattern (in grey) through a single round

authentication

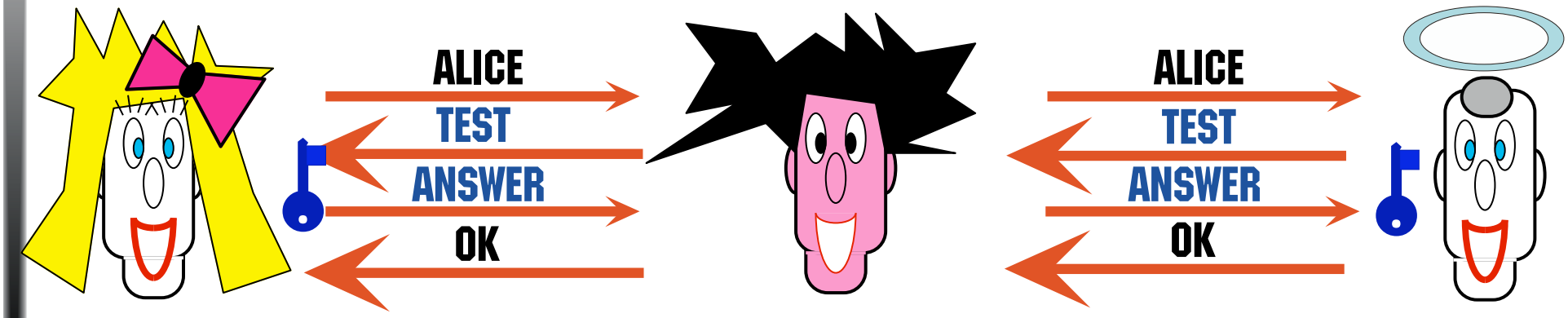
One-Time-Authentication from PRBG

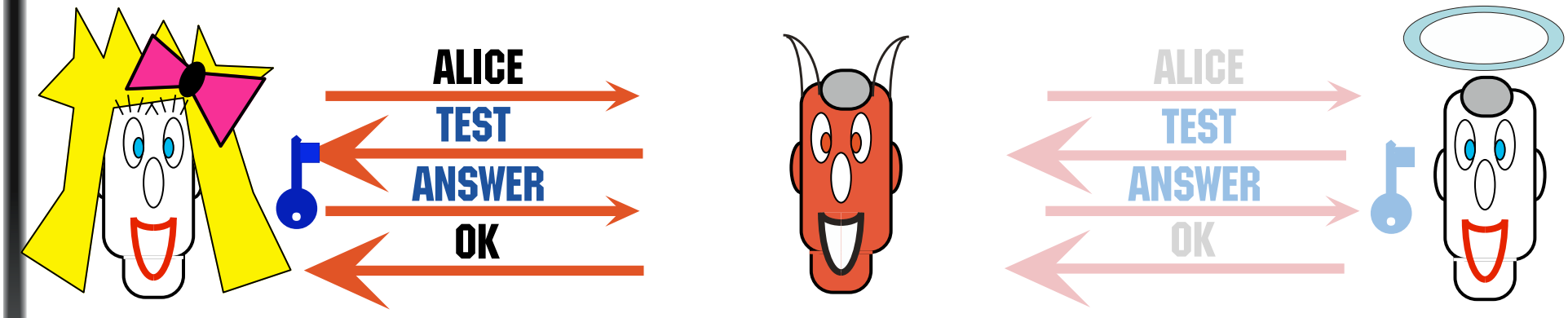


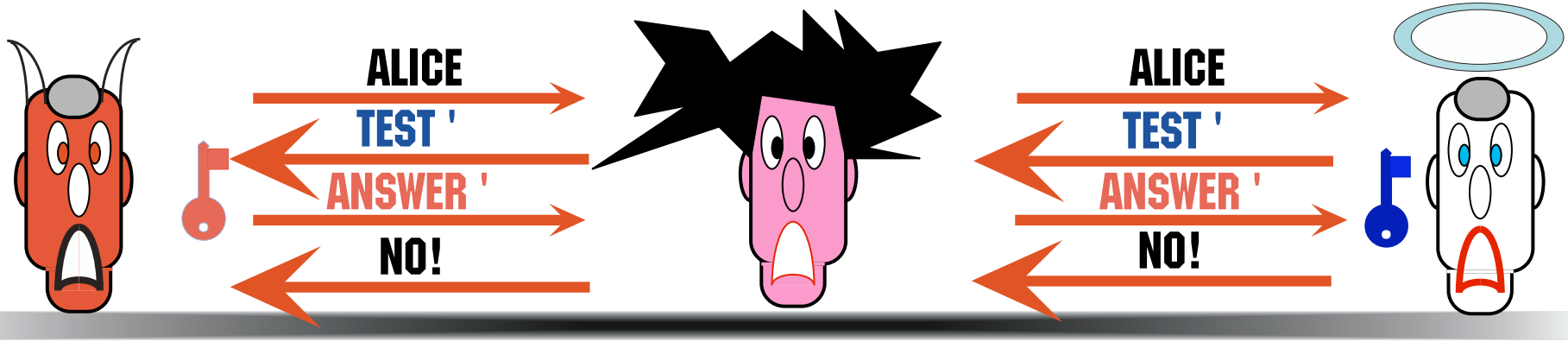
Message Authentication Codes (MACs)

identification

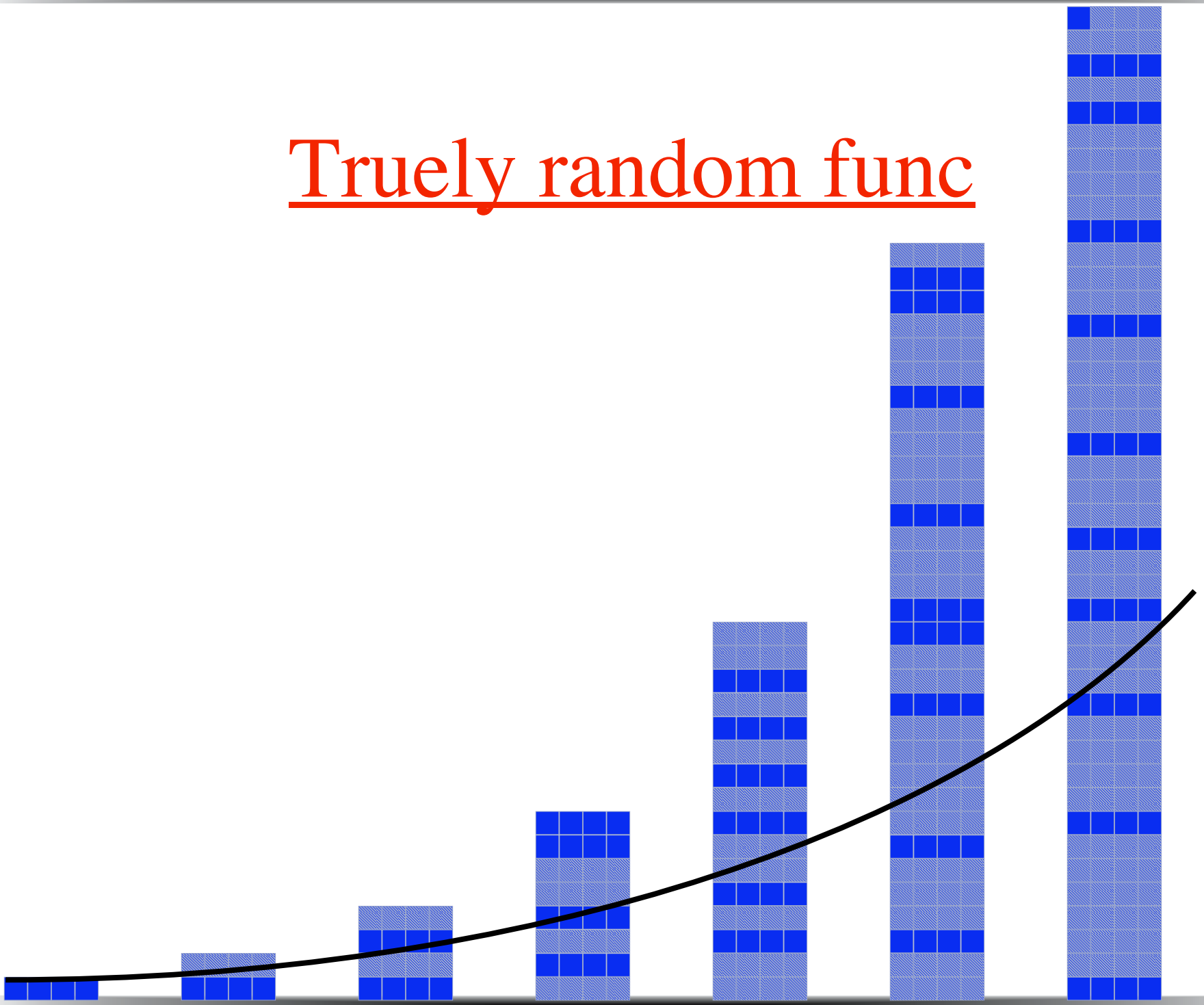
on-line identification



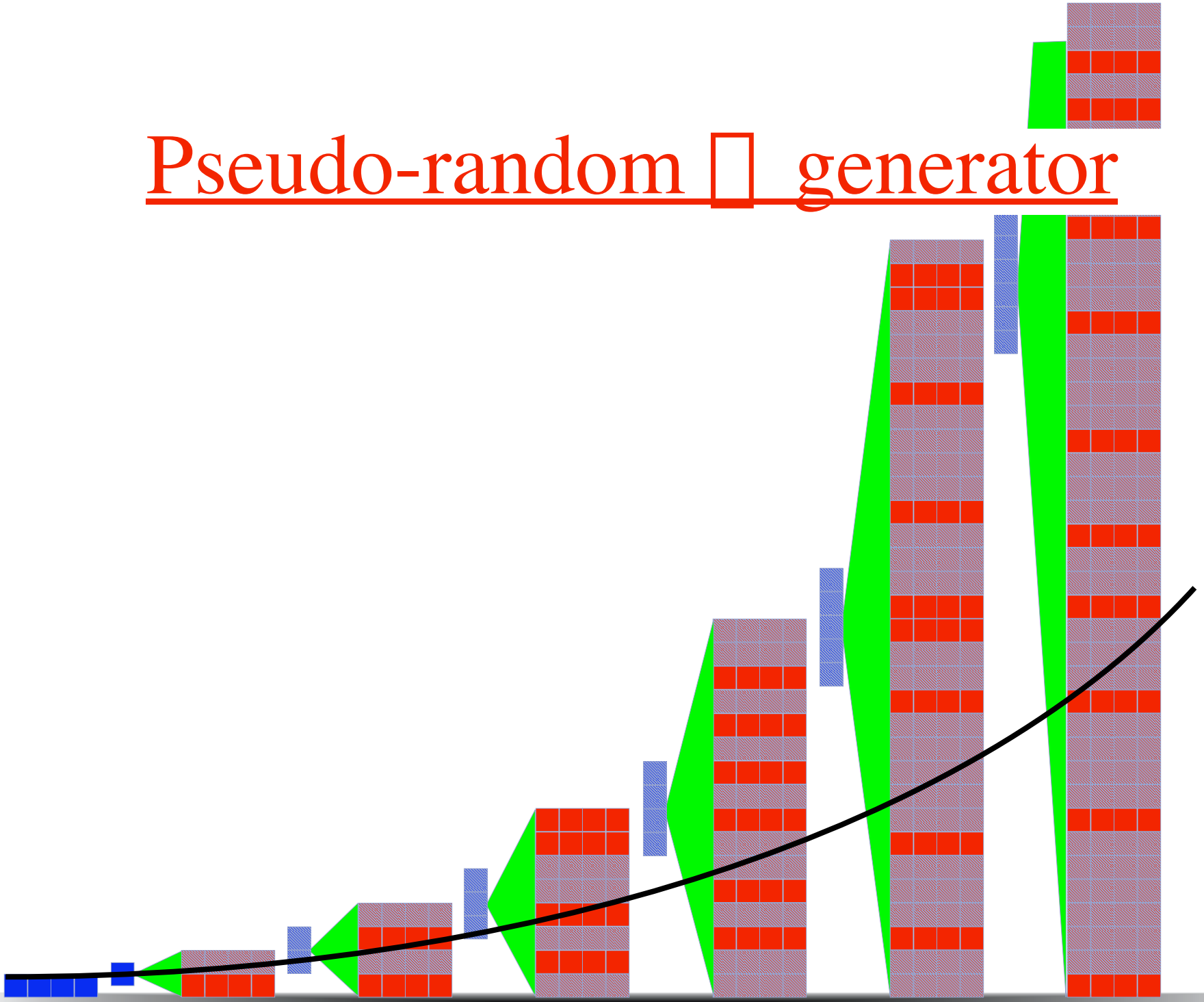




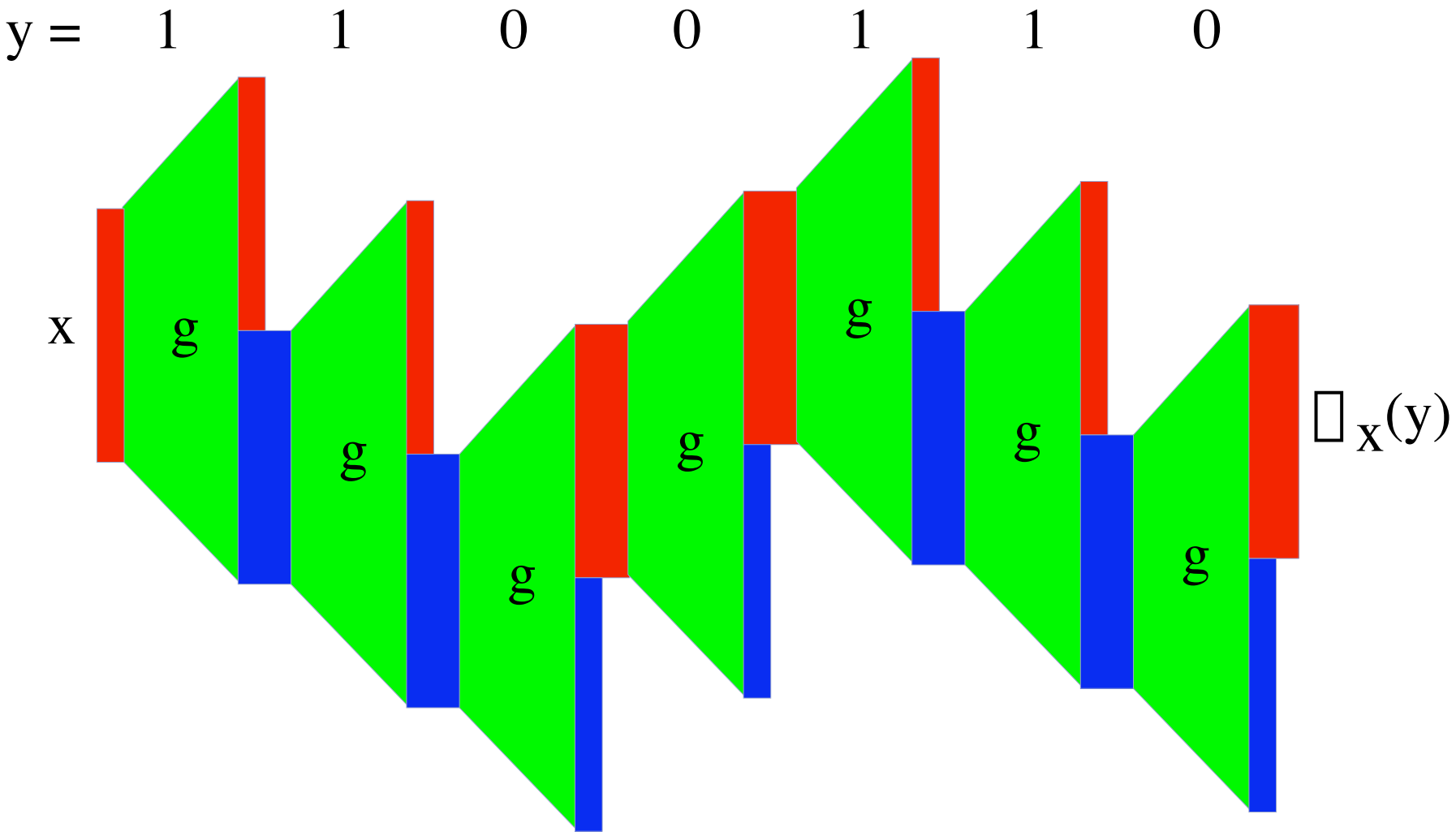
Truely random func

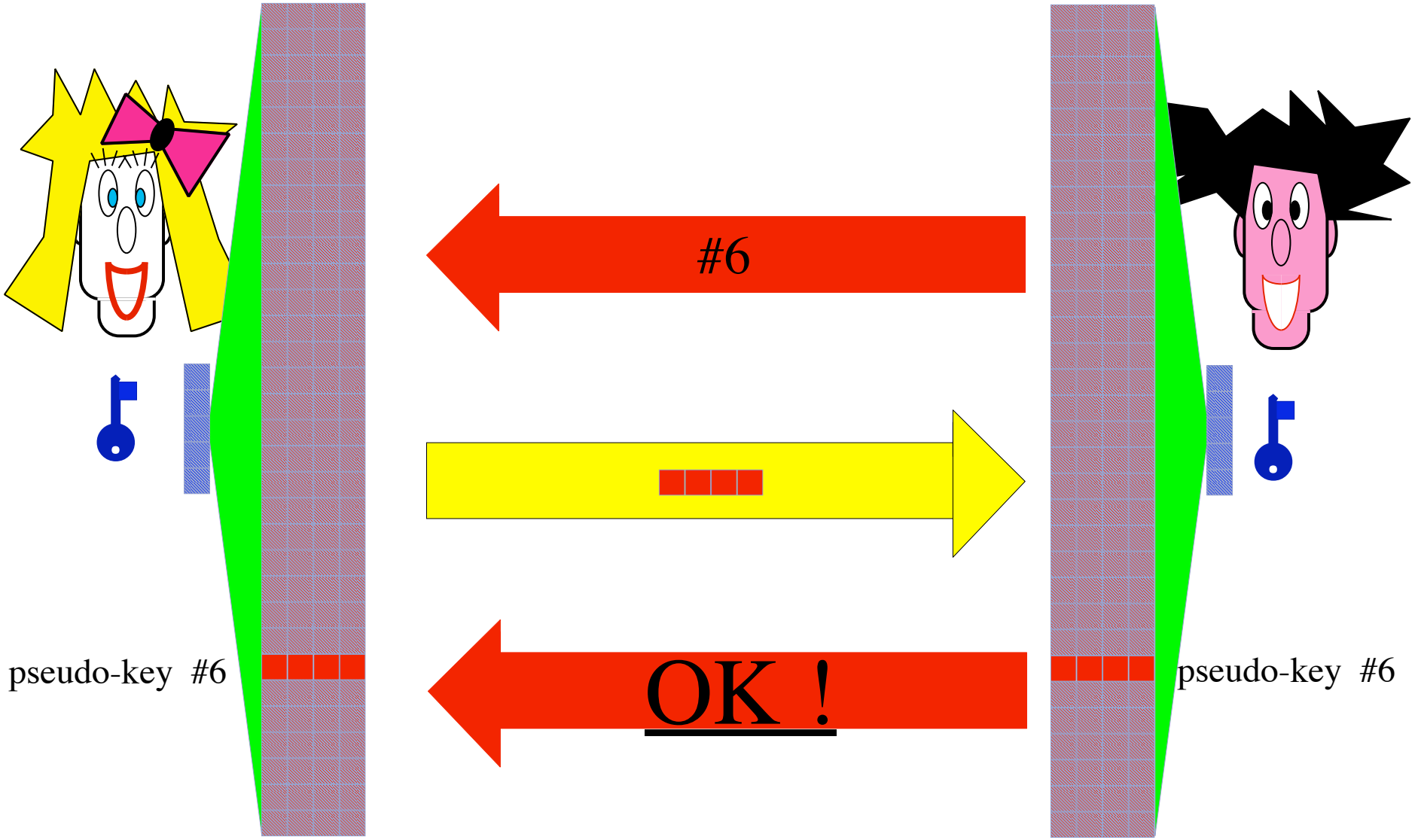


Pseudo-random generator

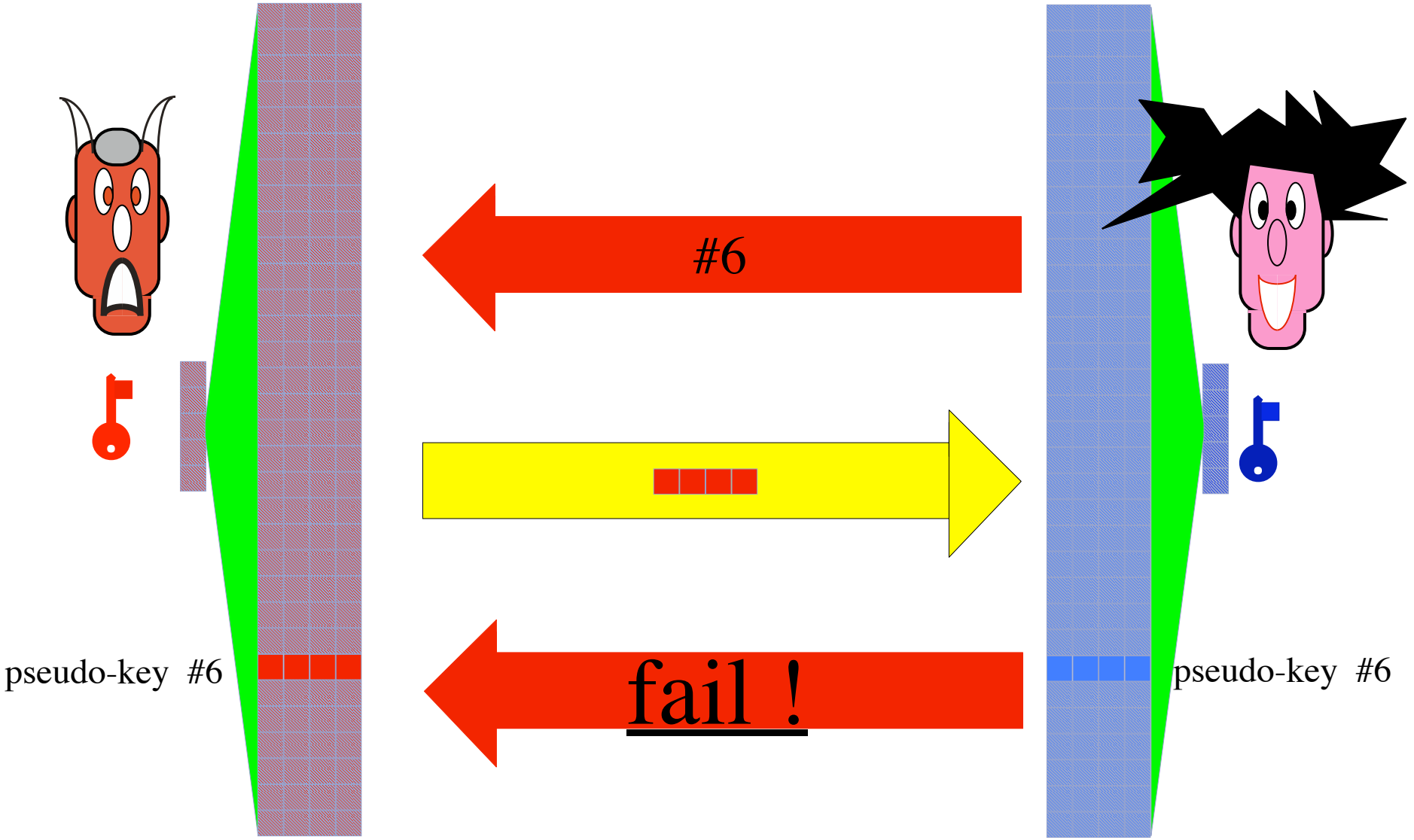


Pseudo-random generator



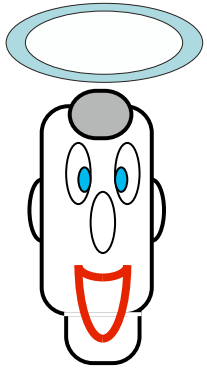


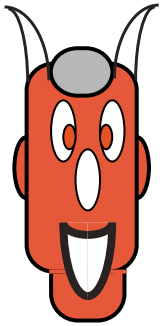
Identification from PR□G

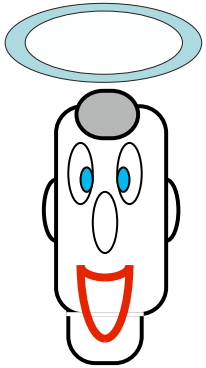


Identification from PR□G

Complexity Theoretical Asymmetric Cryptography







. . . . .

public key distribution

asymmetric encryption

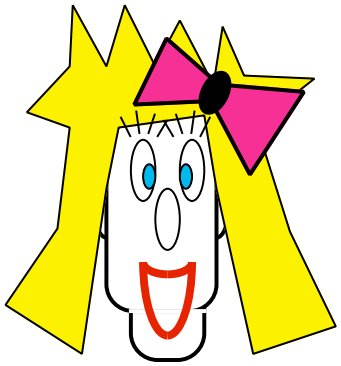
asymmetric authentication

zero-knowledge identification

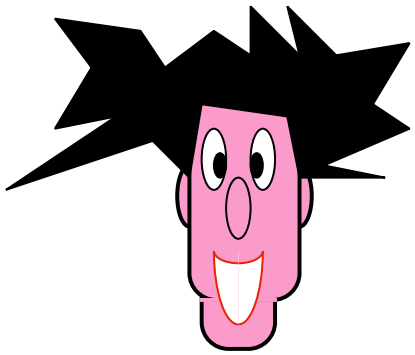
. . . . .

public key distribution

PUBLIC-KEY DISTRIBUTION



p



x:=f(p,a)

y:=f(p,b)

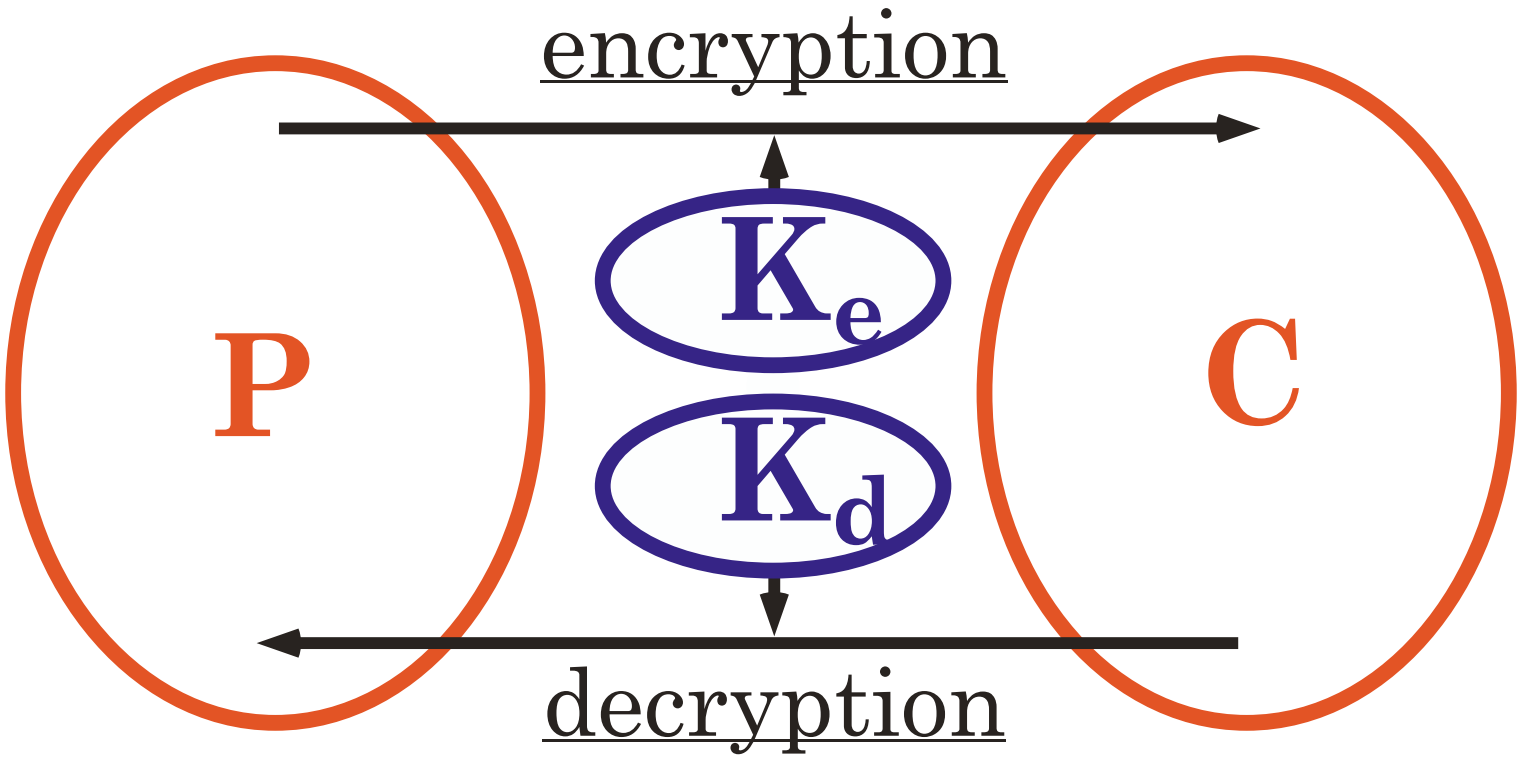
k:=f(y,a)

k:=f(x,b)

f(f(p,a),b)=k=f(f(p,b),a)

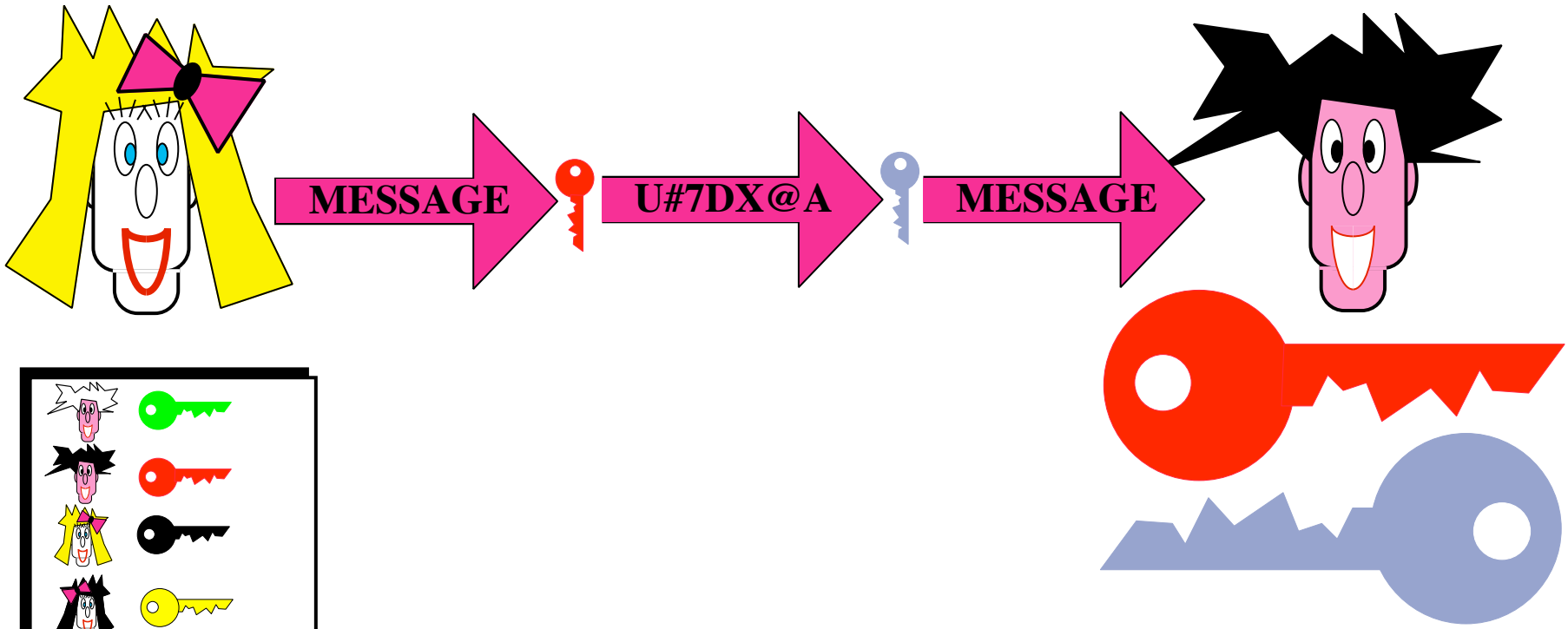
public key encryption

asymmetric encryption
(public-key cryptography)



Complexity Theoretical Security

PUBLIC-KEY CRYPTOGRAPHY



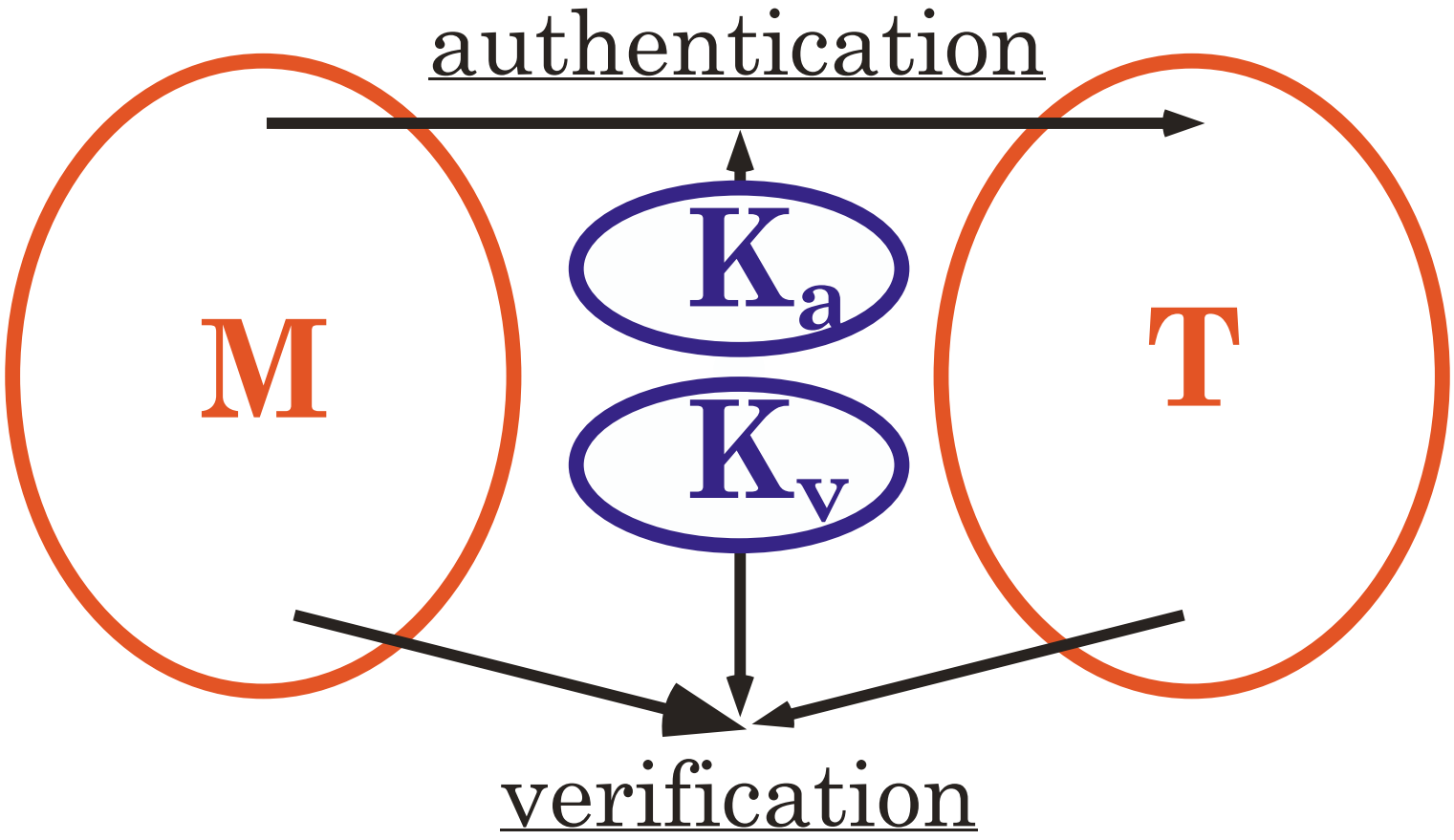
Various PKCS

- RSA: discret root extraction
- ElGamal: discret log
- Meneze-Vanstone: elliptic curves
- McEliece: error correcting codes
- Blum-Goldwasser: factoring
- Ajtai-Dwork: lattice

digital signatures

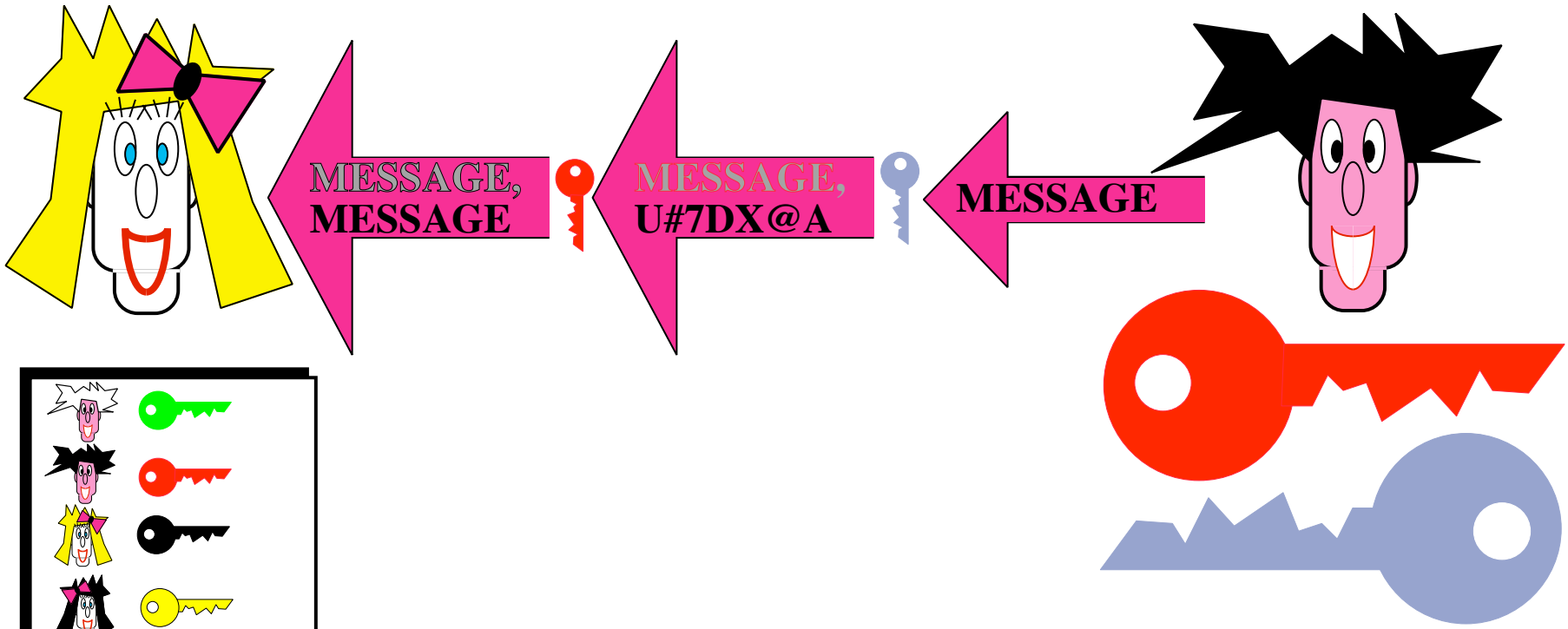
asymmetric authentication

(digital signature schemes)



Complexity Theoretical Security

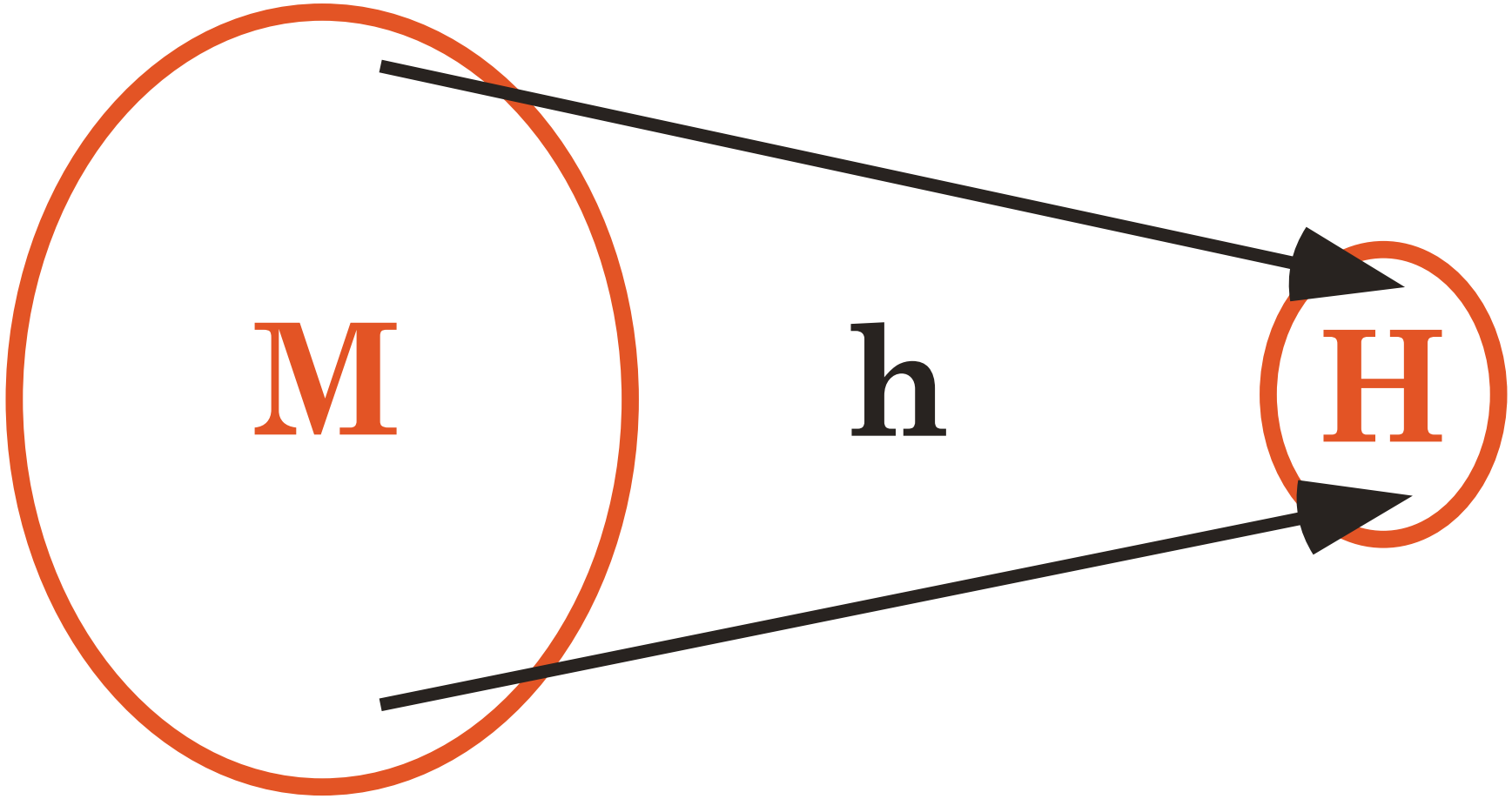
Digital Signature



Various Digital Signatures

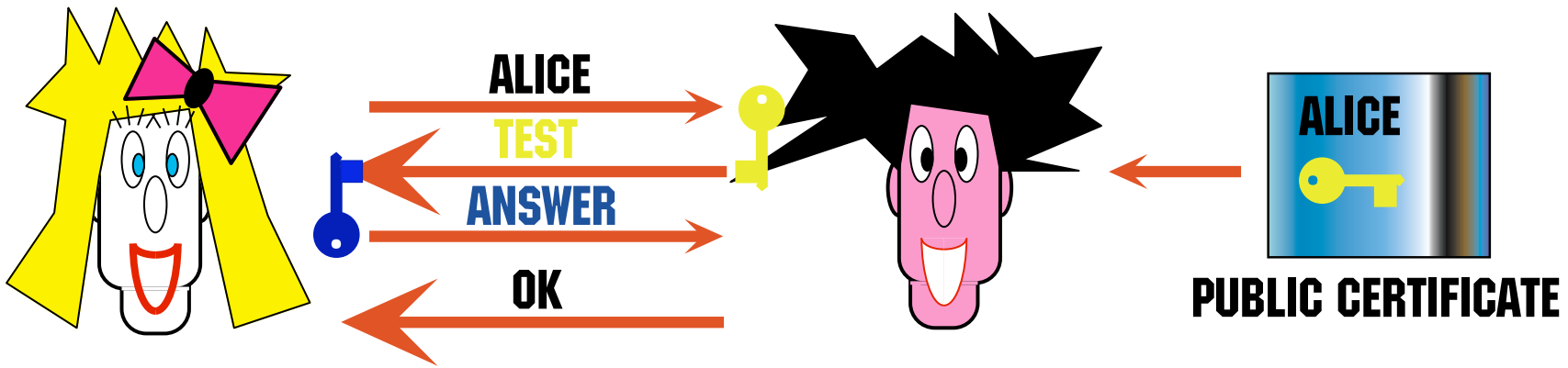
- RSA: discret root extraction
- ElGamal: discret log
- DSS: variant of ElGamal
- Chaum et al: undeniable sign.
- Pfitzman-Waidner: fail-stop sign.

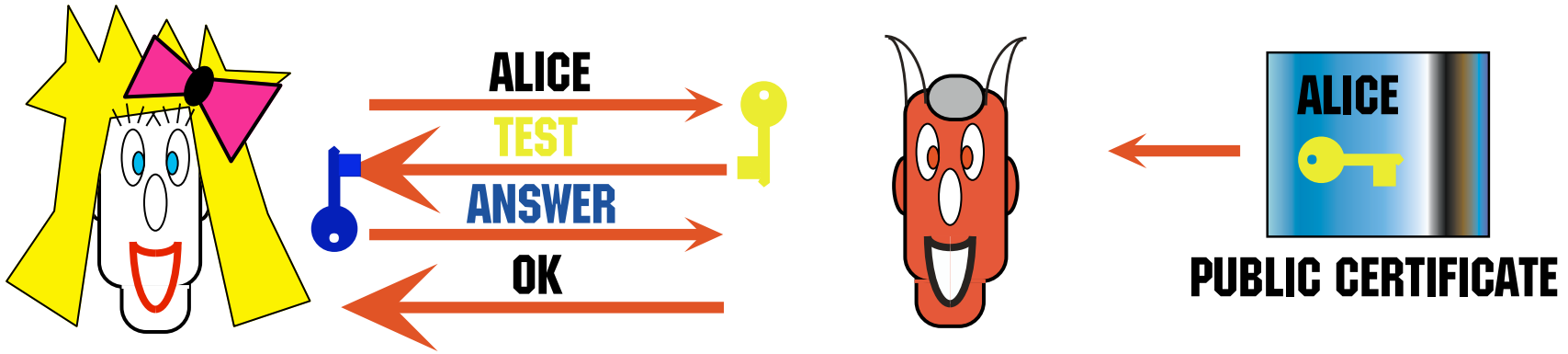
Message Digest
(cryptographic hashing)

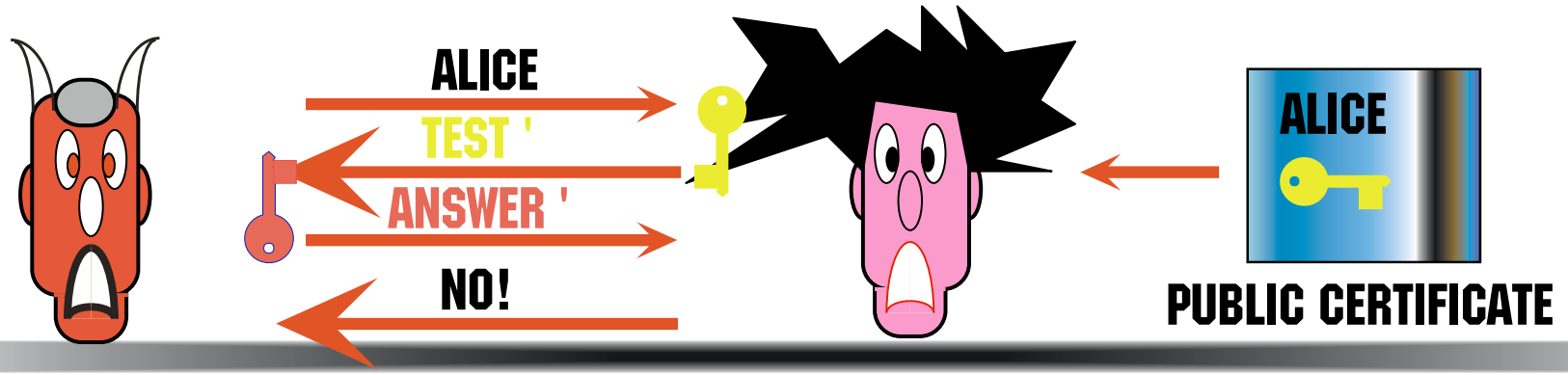


zero-knowledge identification

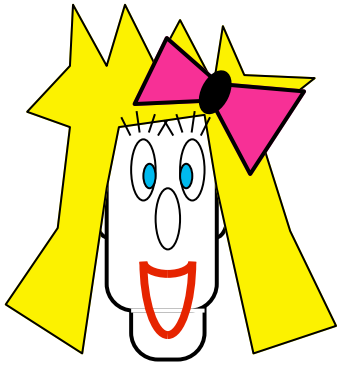
off-line solution

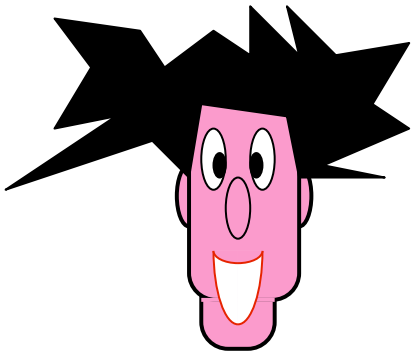






Interactive Proofs and Zero-Knowledge



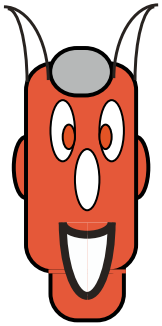


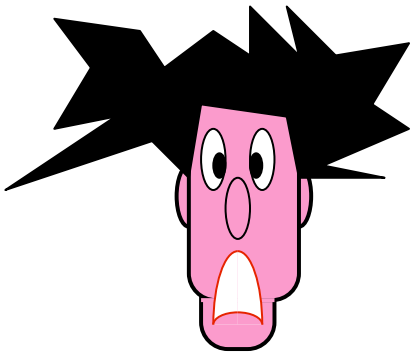
$x \in L$

YES !

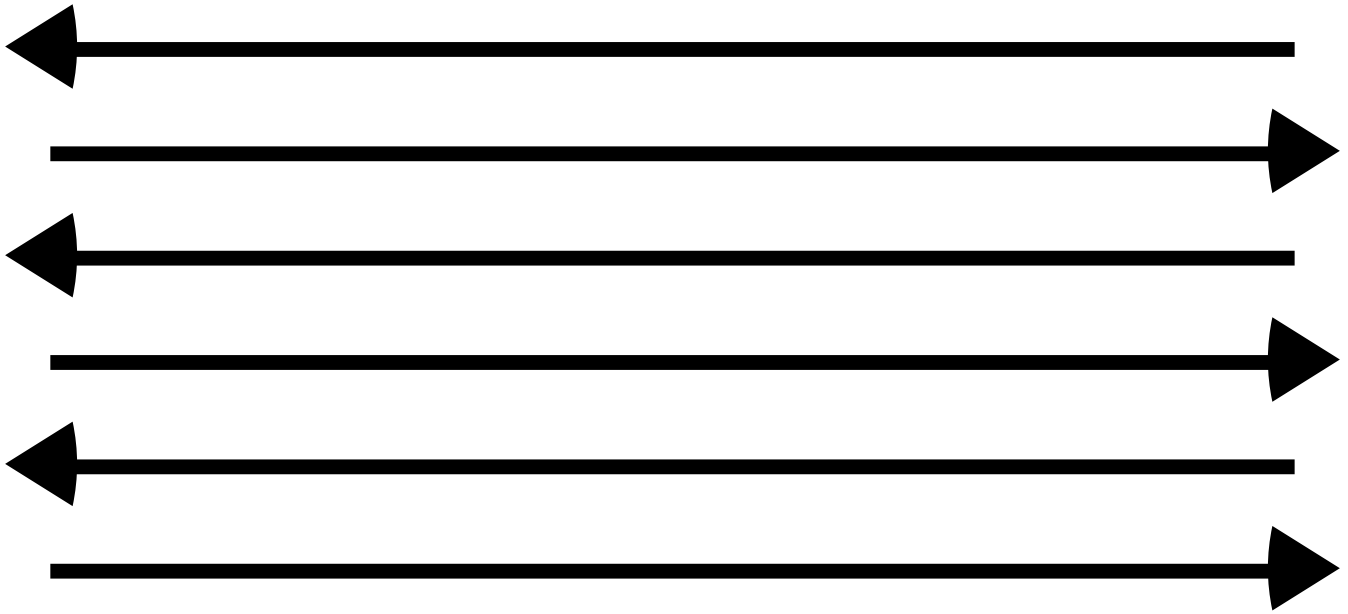
$\forall x \in L \Pr([A,B](x)=YES) \geq 1$

Interactive Proofs and Zero-Knowledge





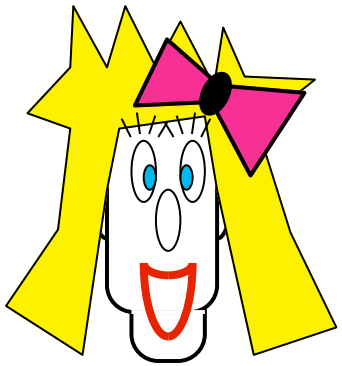
$x \in L$



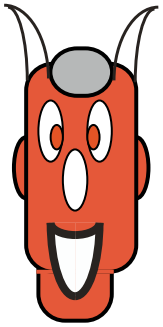
NO !

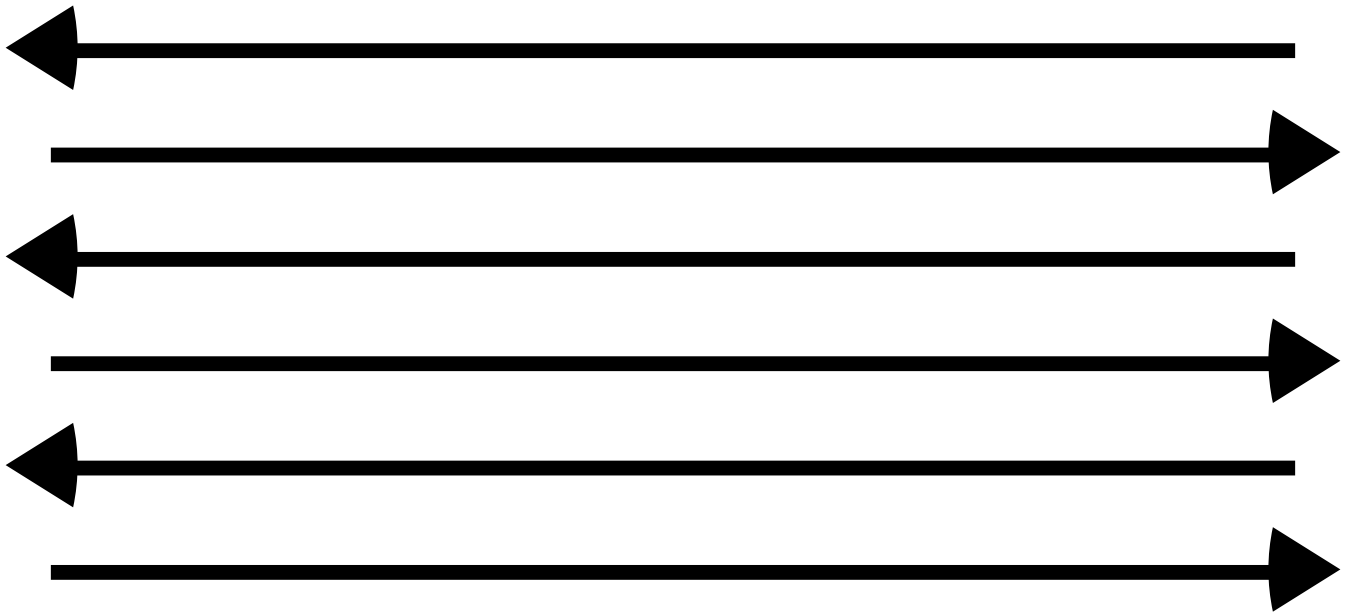
$\forall x \in L \ \forall D \ \Pr([D,B](x)=YES) \geq 0$

Interactive Proofs and Zero-Knowledge



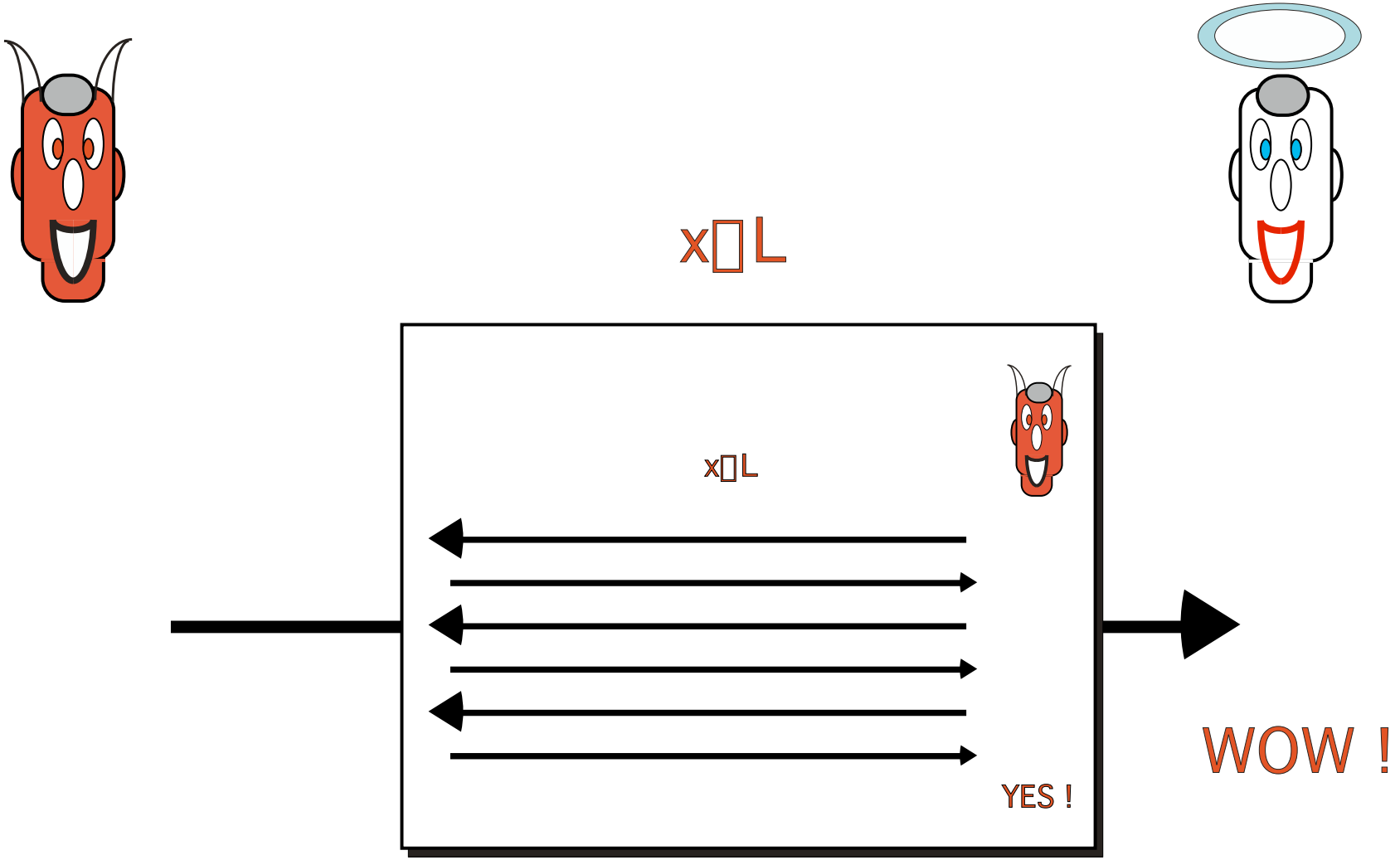
$x \square L$



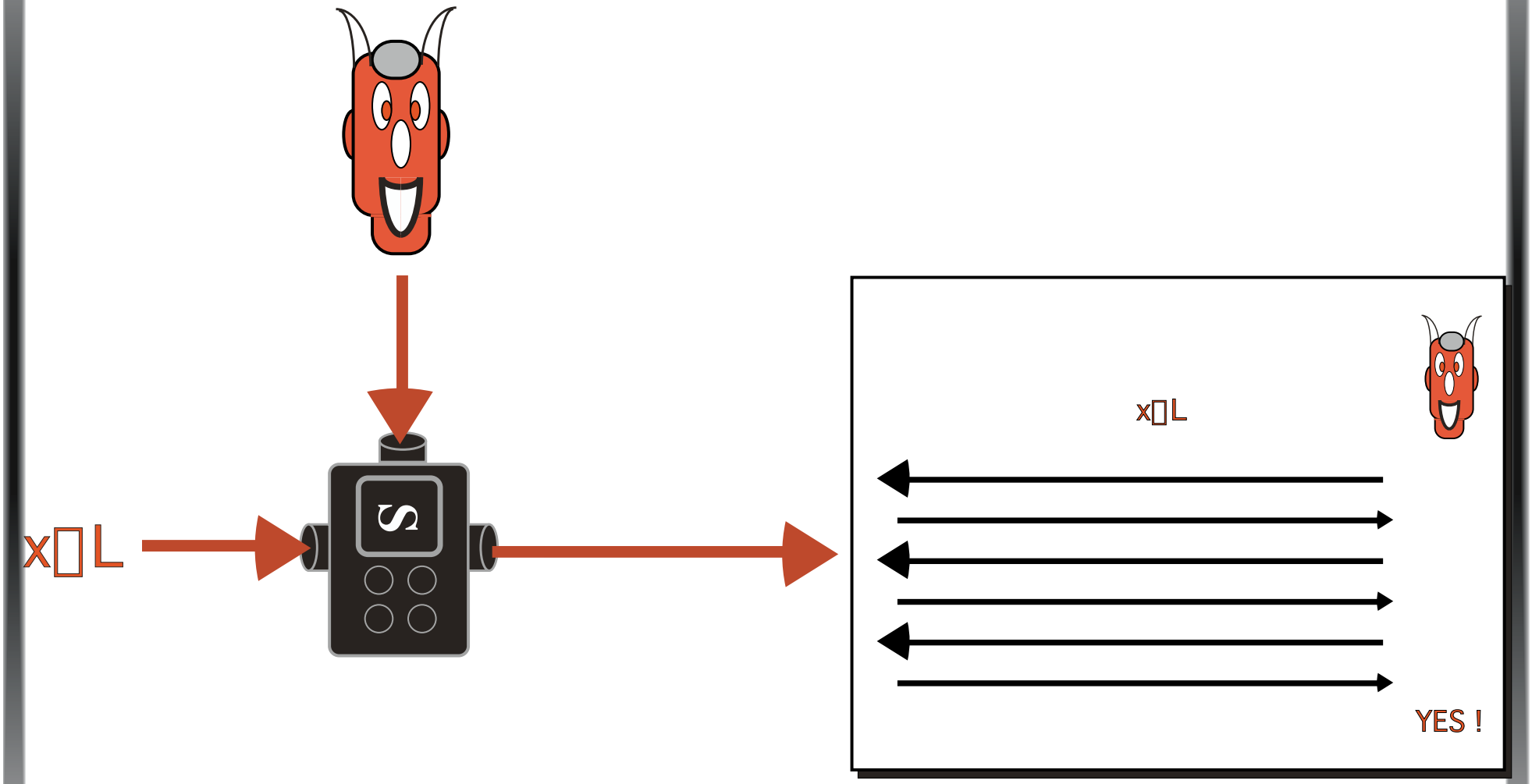


YES !

Interactive Proofs and NOT Zero-Knowledge



Zero-Knowledge by Simulator



$$\forall_{eff} D \; \exists_{eff} S_D \; \forall x \in L \; view_D[A,D](x) = S_D(x)$$

CS547A
Cryptography and Data Security

Lecture 02

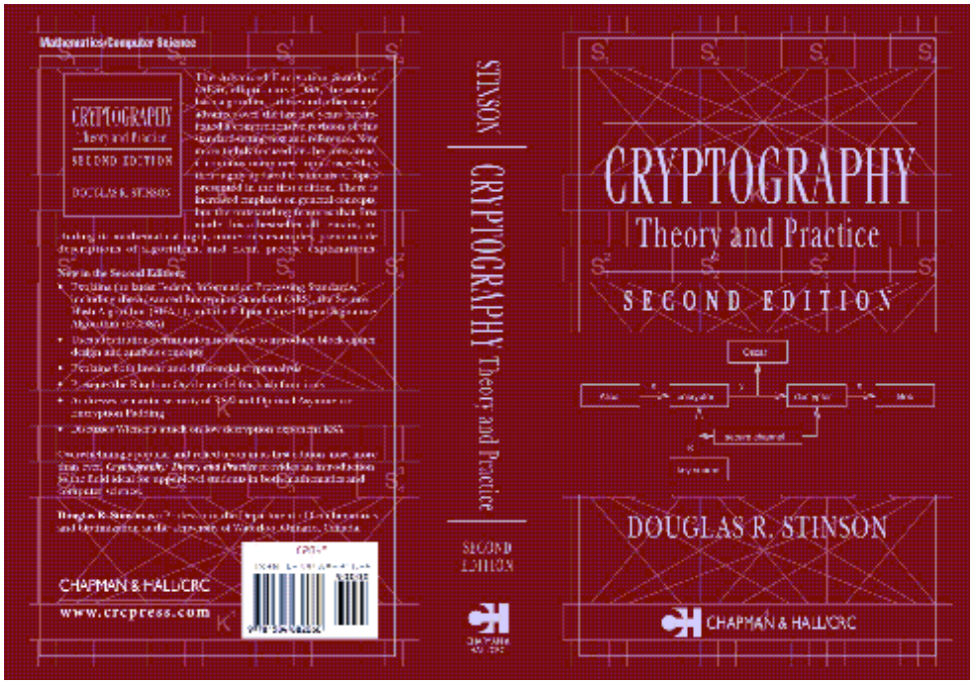
Claude Crépeau

School of Computer Science
McGill University

Mandatory Material

.....

- Class notes (course web page)
- Maple™ software
- Stinson's book

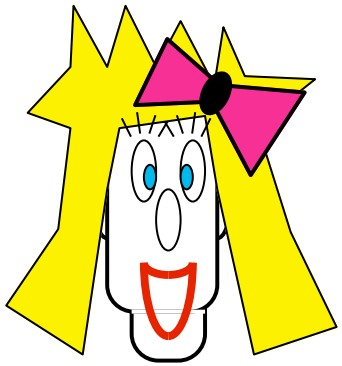


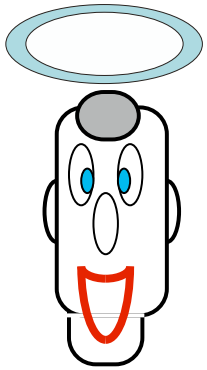
Evaluation

.....

- Theoretical exercices : 30%
- Maple™ exercices : 20%
- FINAL EXAM : 50%

.....





CIAO !