COMP 102A, Lecture 16

Introduction to Cryptography II

COMP 102A, Lecture 16

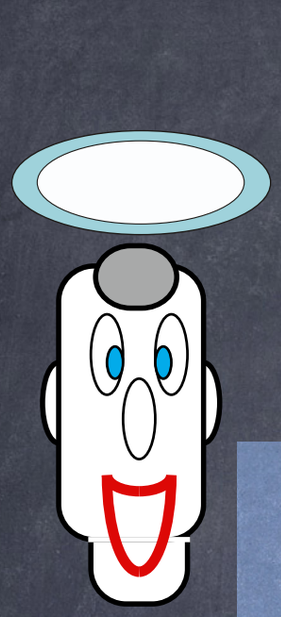
DONE	IN PROGRESS	TO DO	GIVE UP	
2013/01/08				
tasks security	**ENCRYPTION**	**AUTHENTICATION**	**IDENTIFICATION**	
SYMMETRIC INFORMATION THEORY	Vernam: ONE-TIME PAD	Wegman-Carter Universal Hash Functions	simple examples	Quantum Key Distribution
SYMMETRIC COMPLEXITY THEORY	**from PRBG** **from PRFG** DES,AES,etc	from PRBG from PRFG DES,AES,etc	from PRBG from PRFG DES,AES,etc	
ASYMMETRIC COMPLEXITY THEORY	RSA, El Gammal, Blum-	RSA, DSA, etc	Guilloux-Quisquater, Schnor, etc.	Quantum Factoring

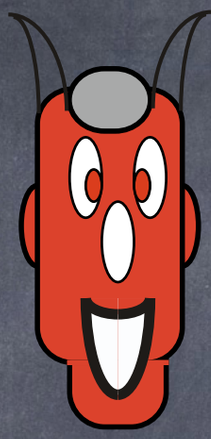
Complexity

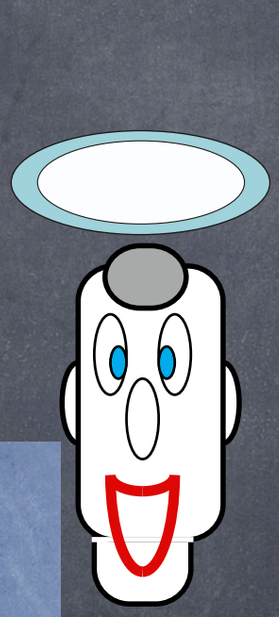
Theoretical

Cryptography

Complexity Theoretical Symmetric Cryptography







.....

Encryption

Authentication

Identification

.....

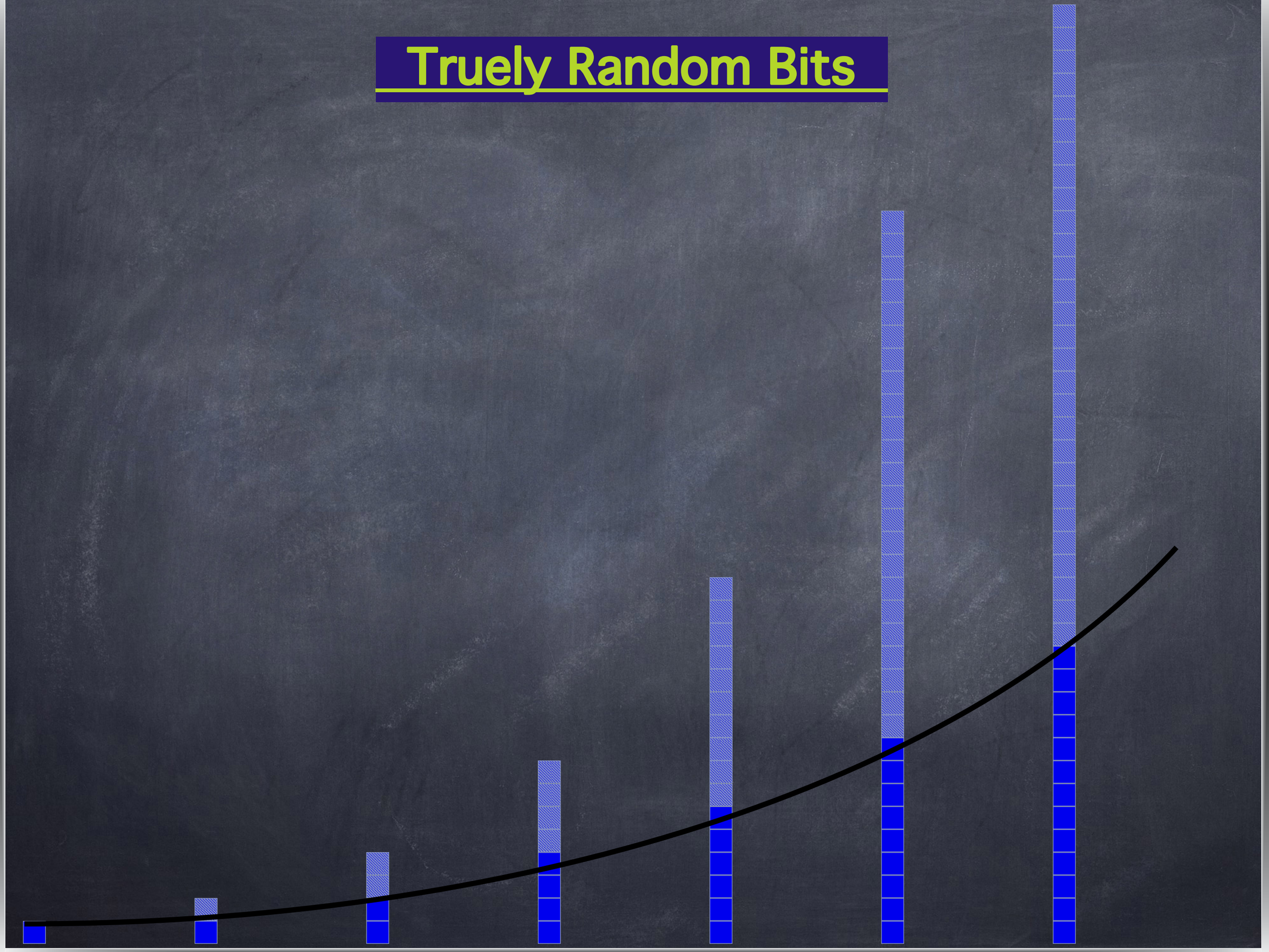
Pseudo-random Bit Generator

Manuel Blum

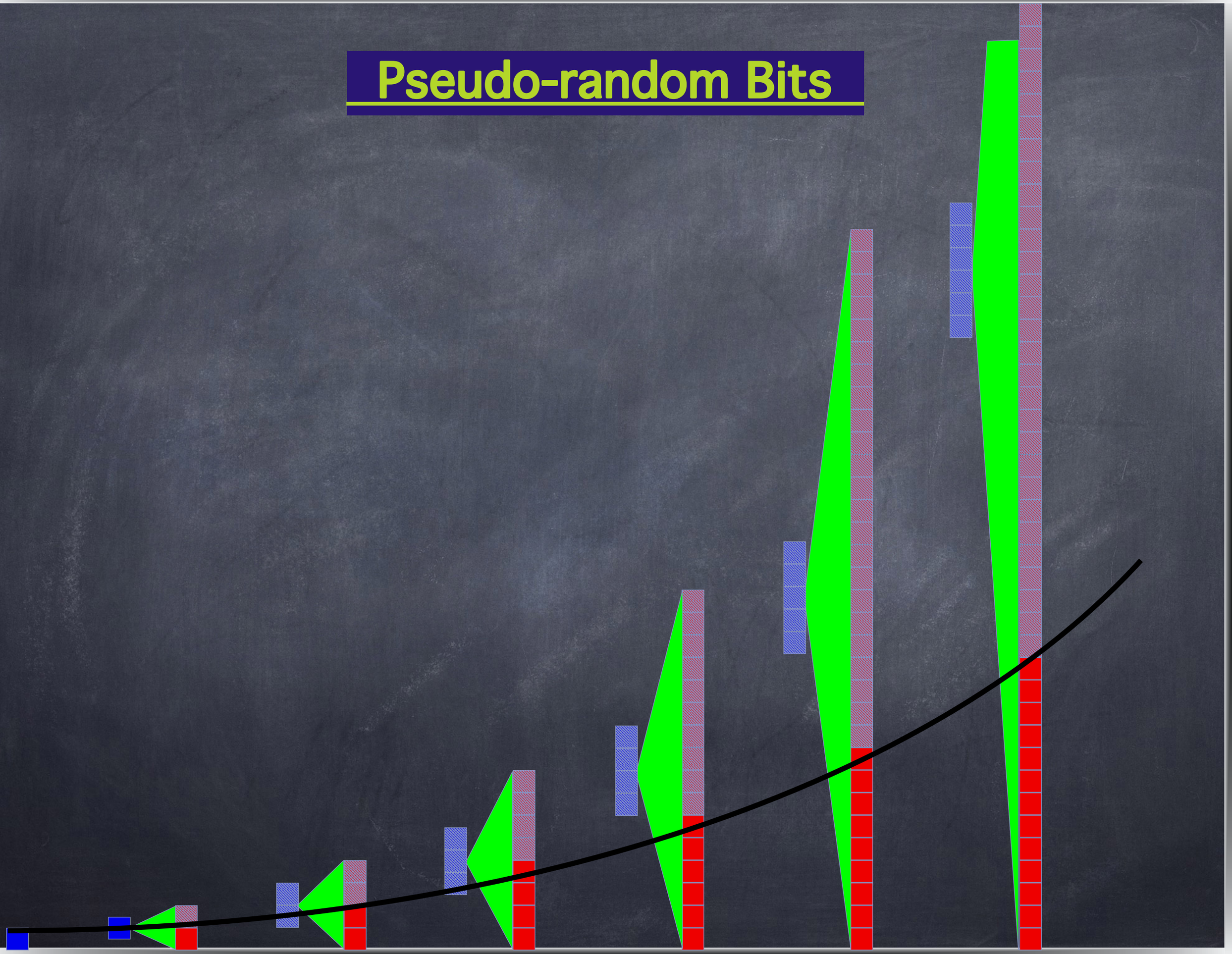
Silvio Micali

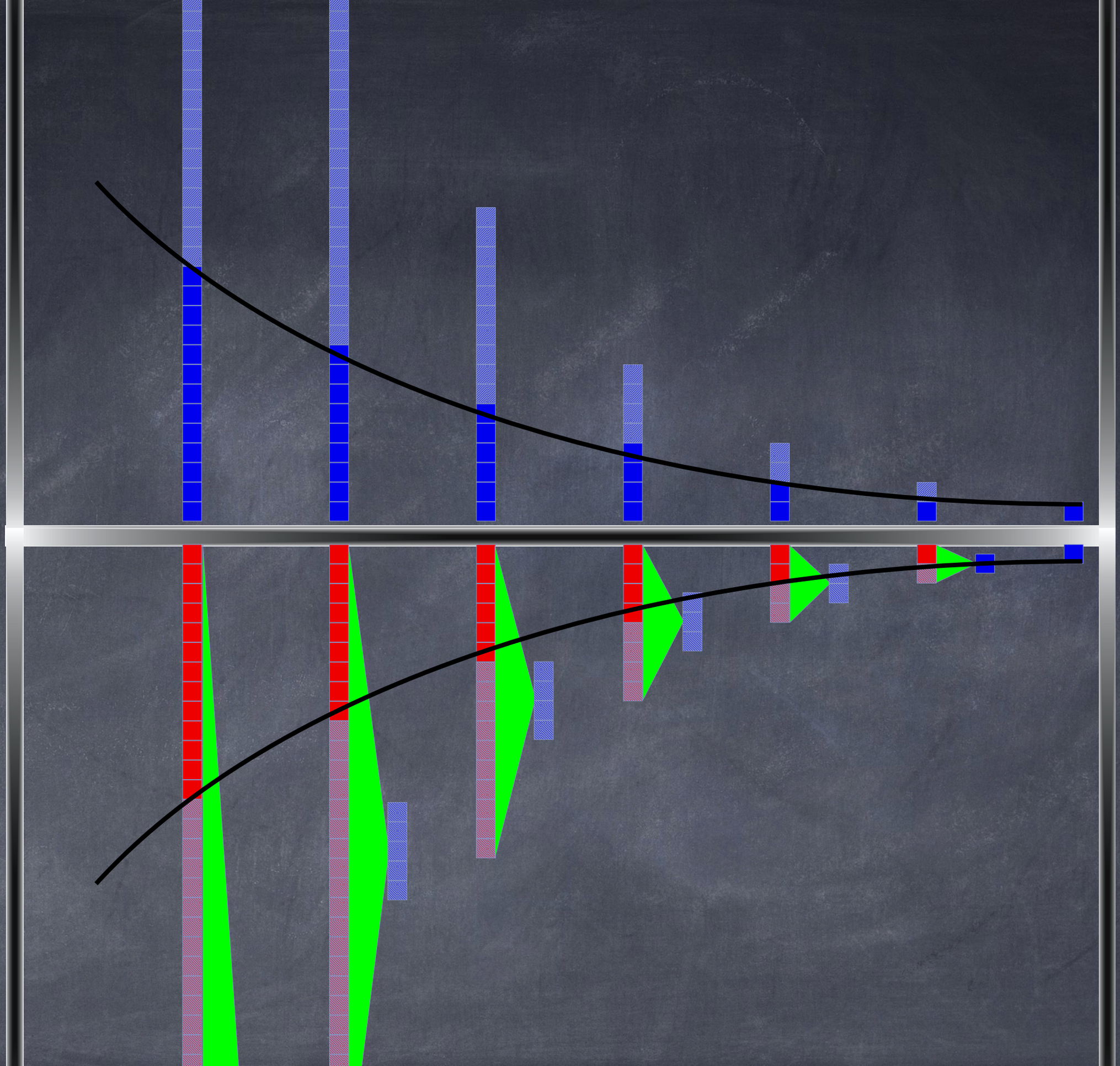
RANDOM x g g(x) SEEMS RANDOM

Truely Random Bits



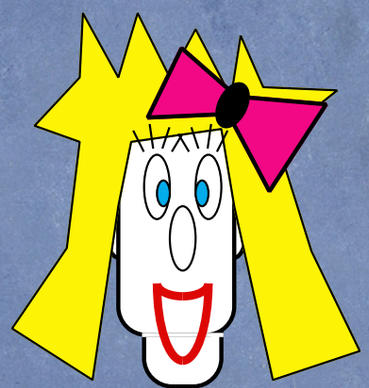
Pseudo-random Bits

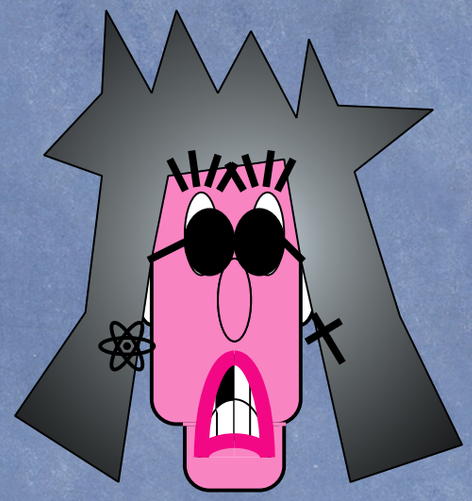


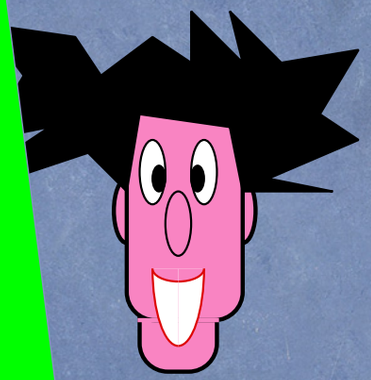


Encryption

Stream Cipher from Pseudo-random Bits



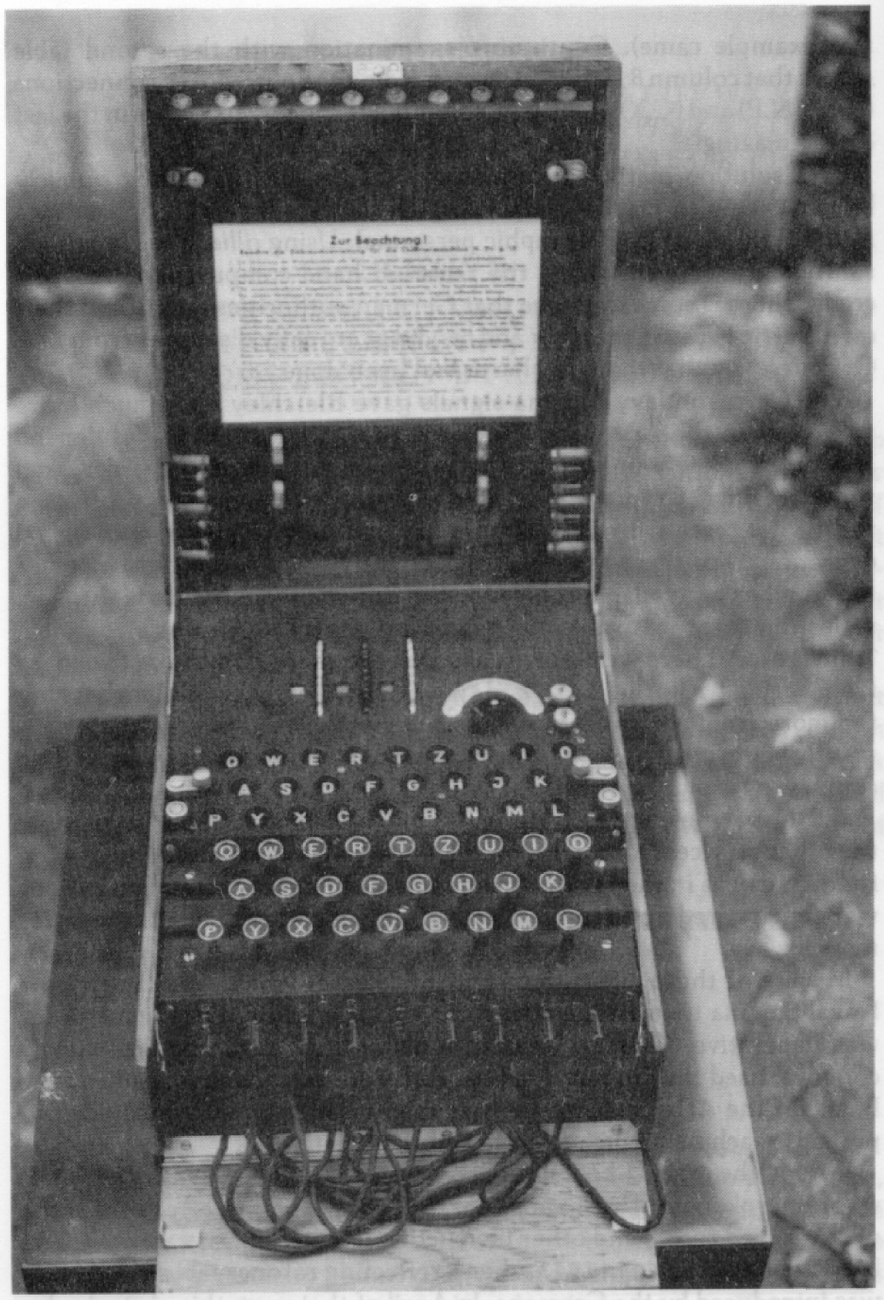




pseudo-key ⊕ cleartext = ciphertext

ciphertext ⊕ pseudo-key = cleartext

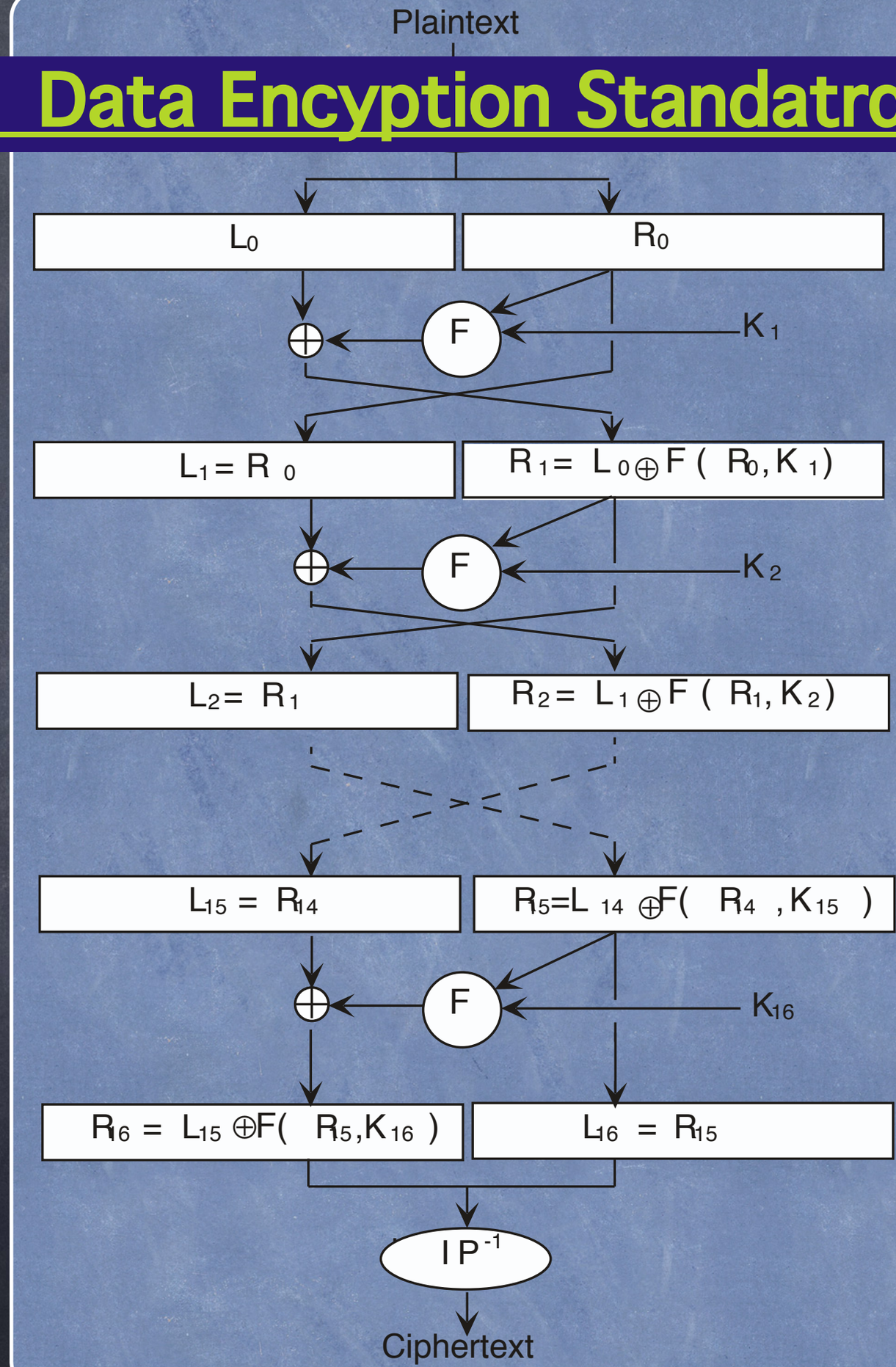
The Enigma Machine



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

Arthur Scherbius

Data Encyption Standatrd



DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

IBM

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Advanced Encyption Standatrd

Joan Daemen

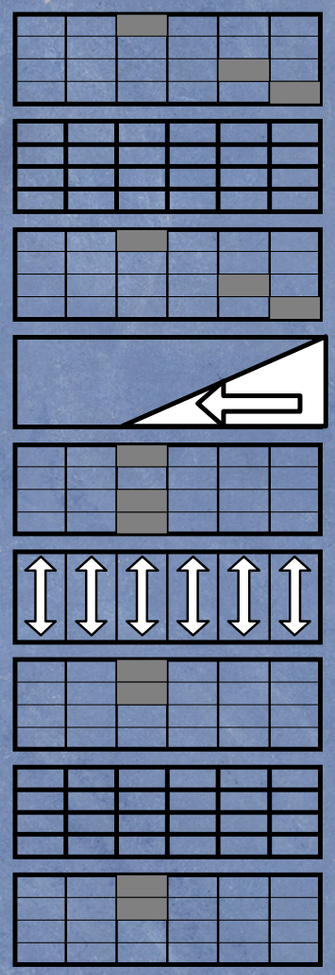
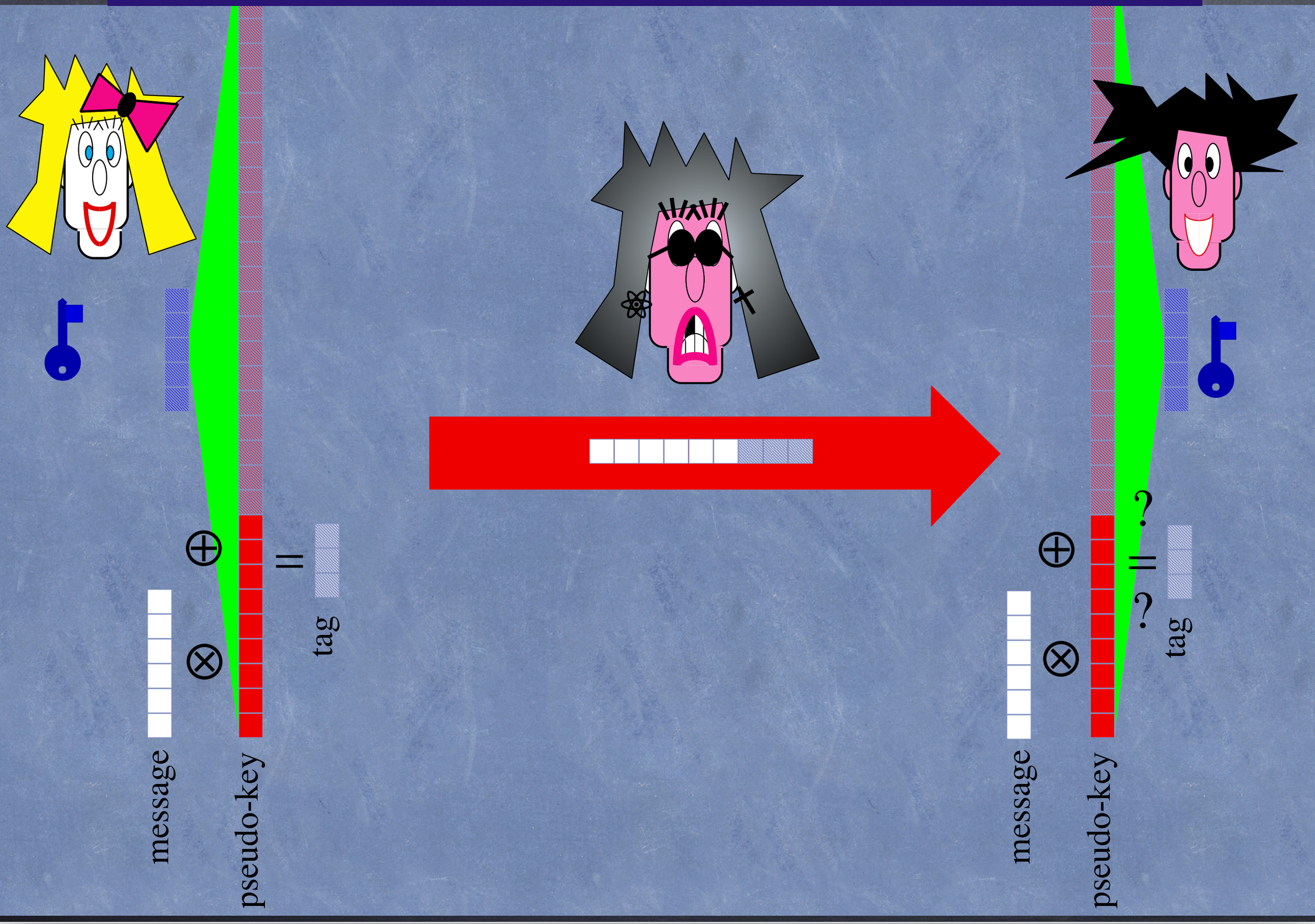


Figure 7: Propagation of activity pattern (in grey) through a single round

Vincent Rijmen

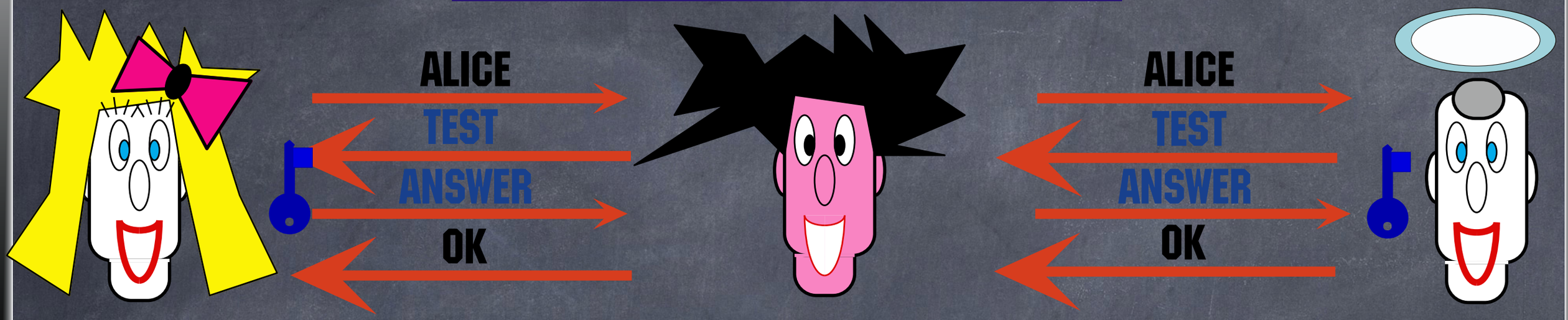
authentication

Authentication from Pseudo-random Bits

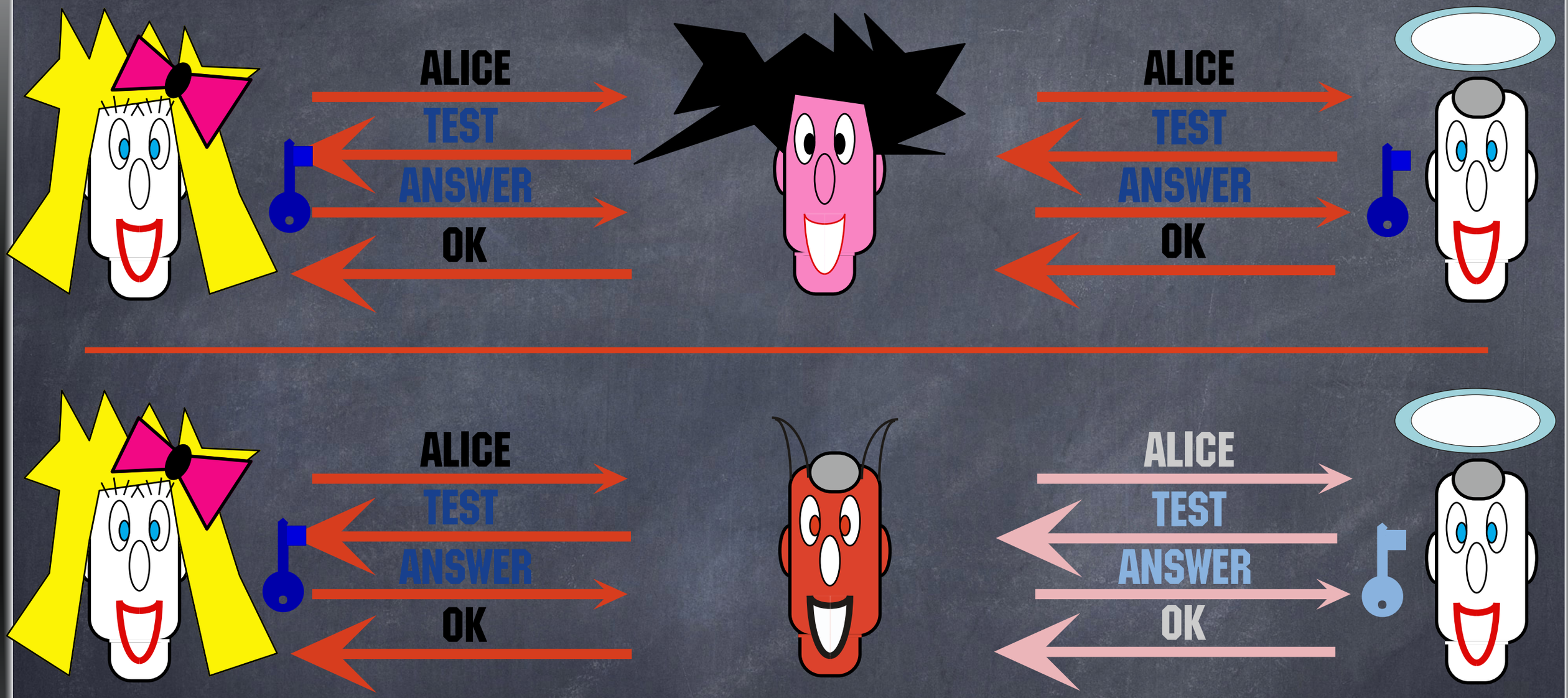


identification

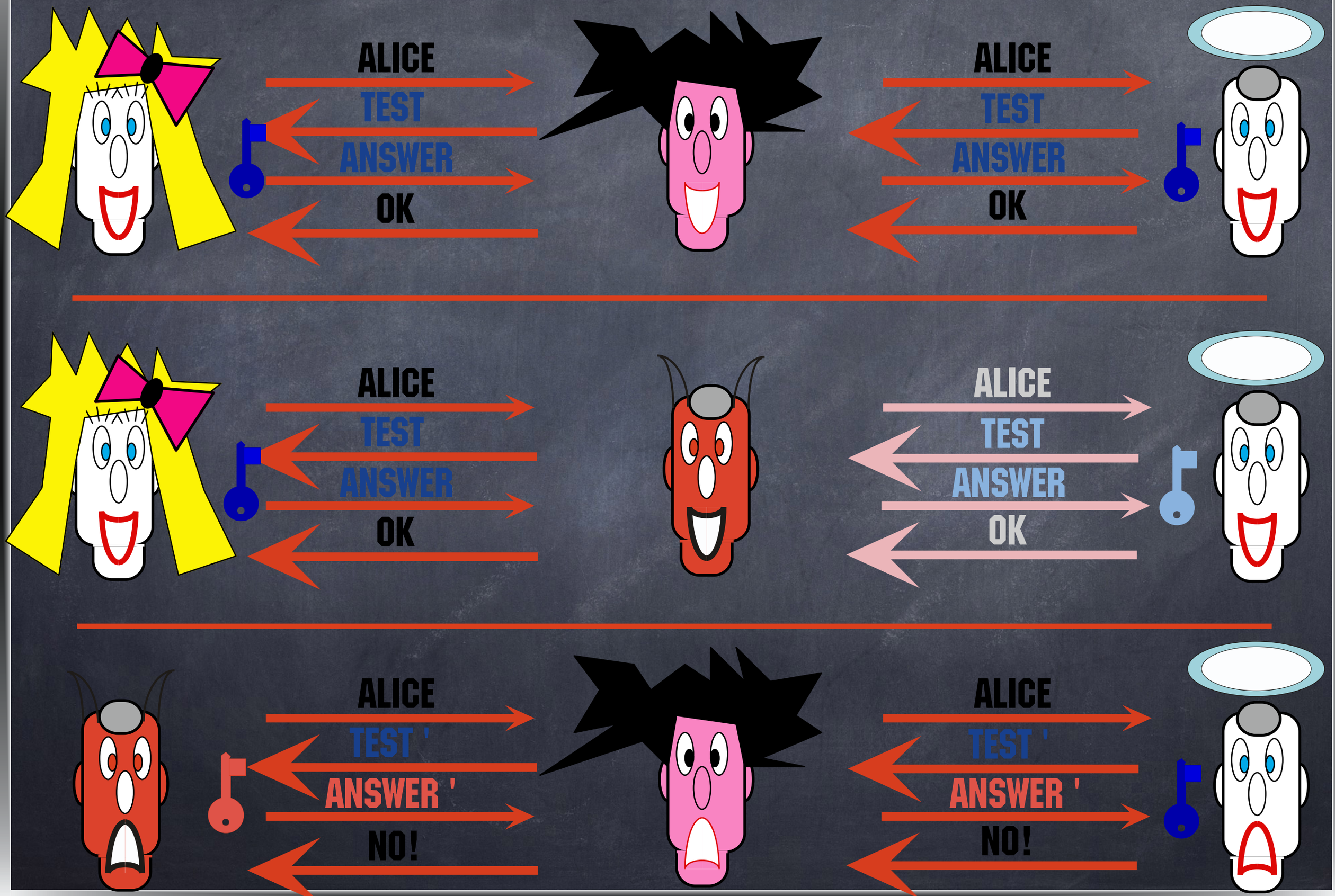
On-line Identification



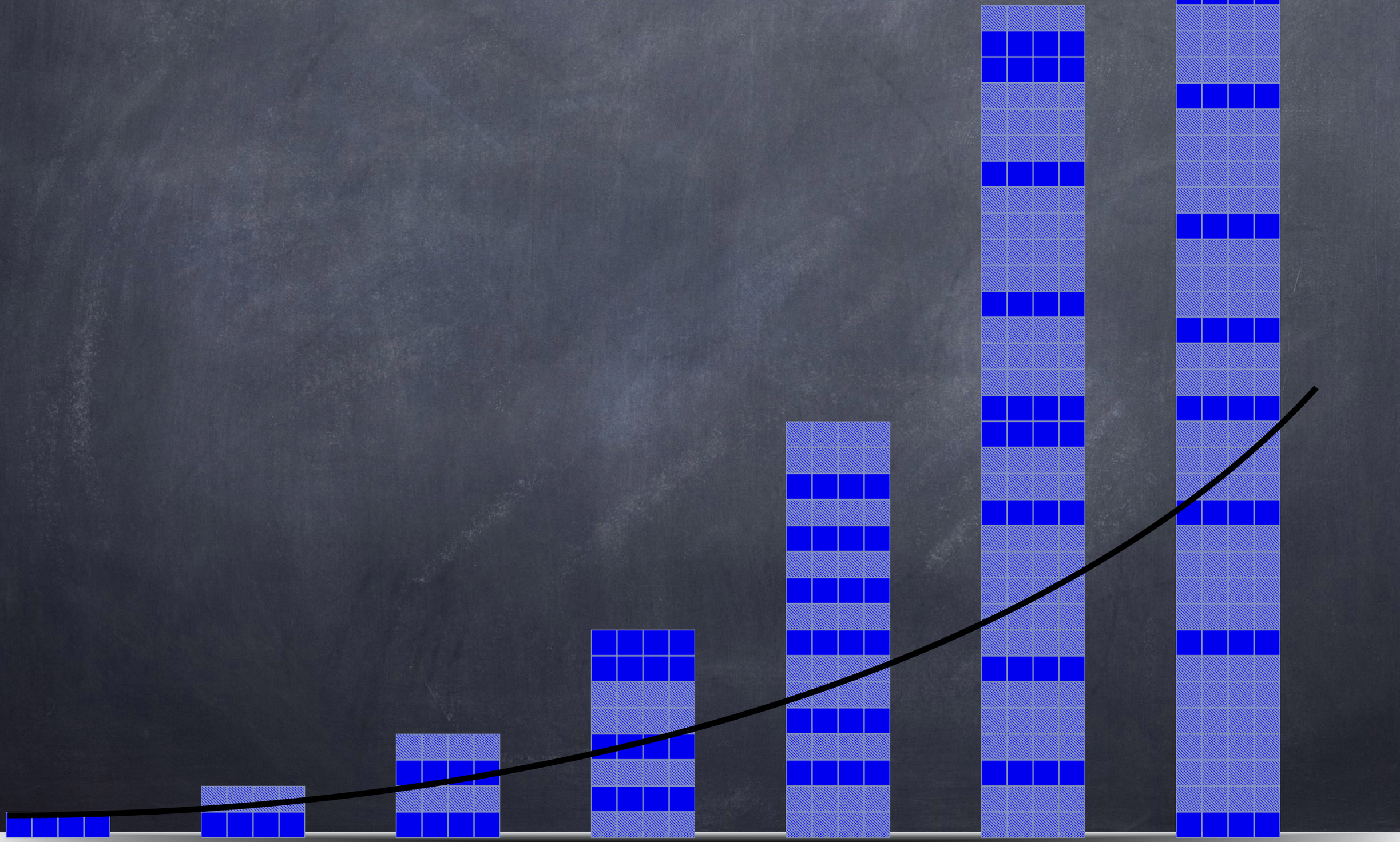
On-line Identification



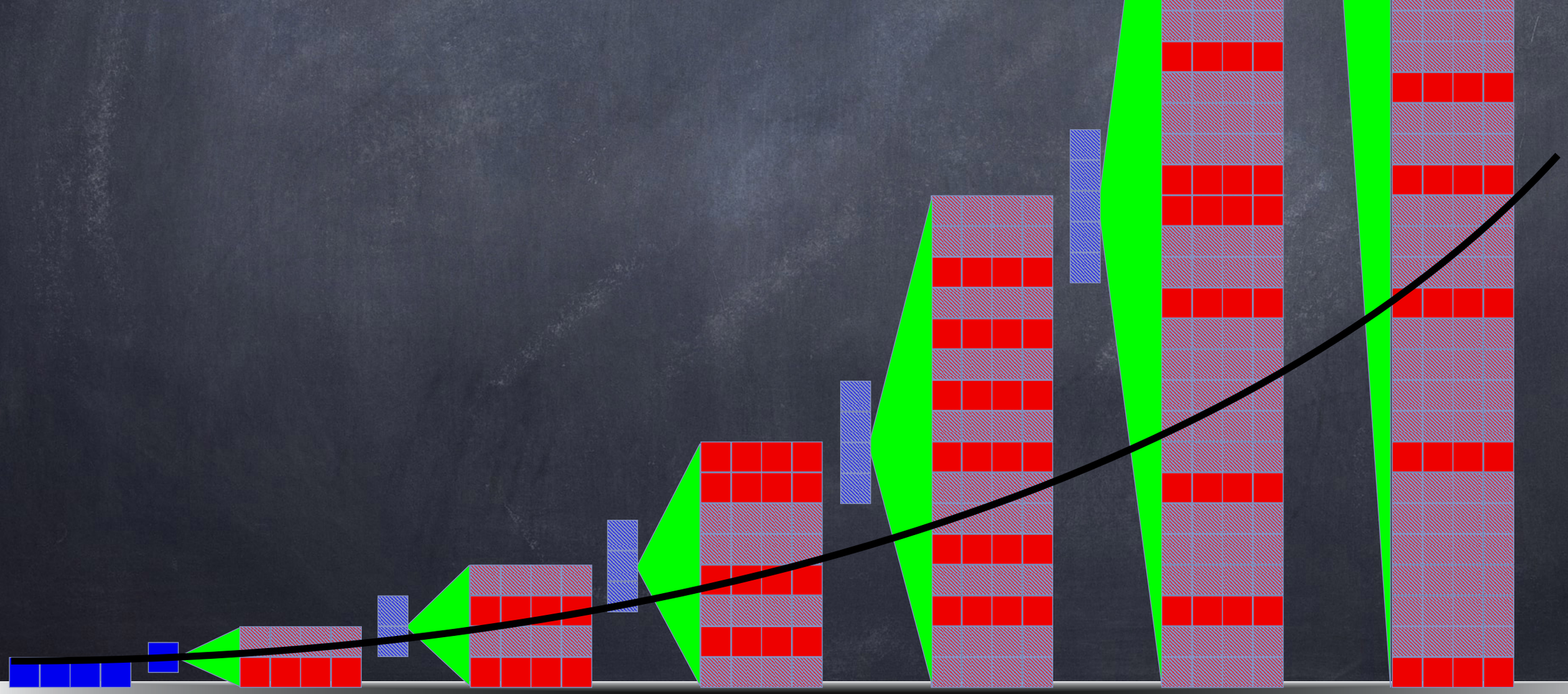
On-line Identification

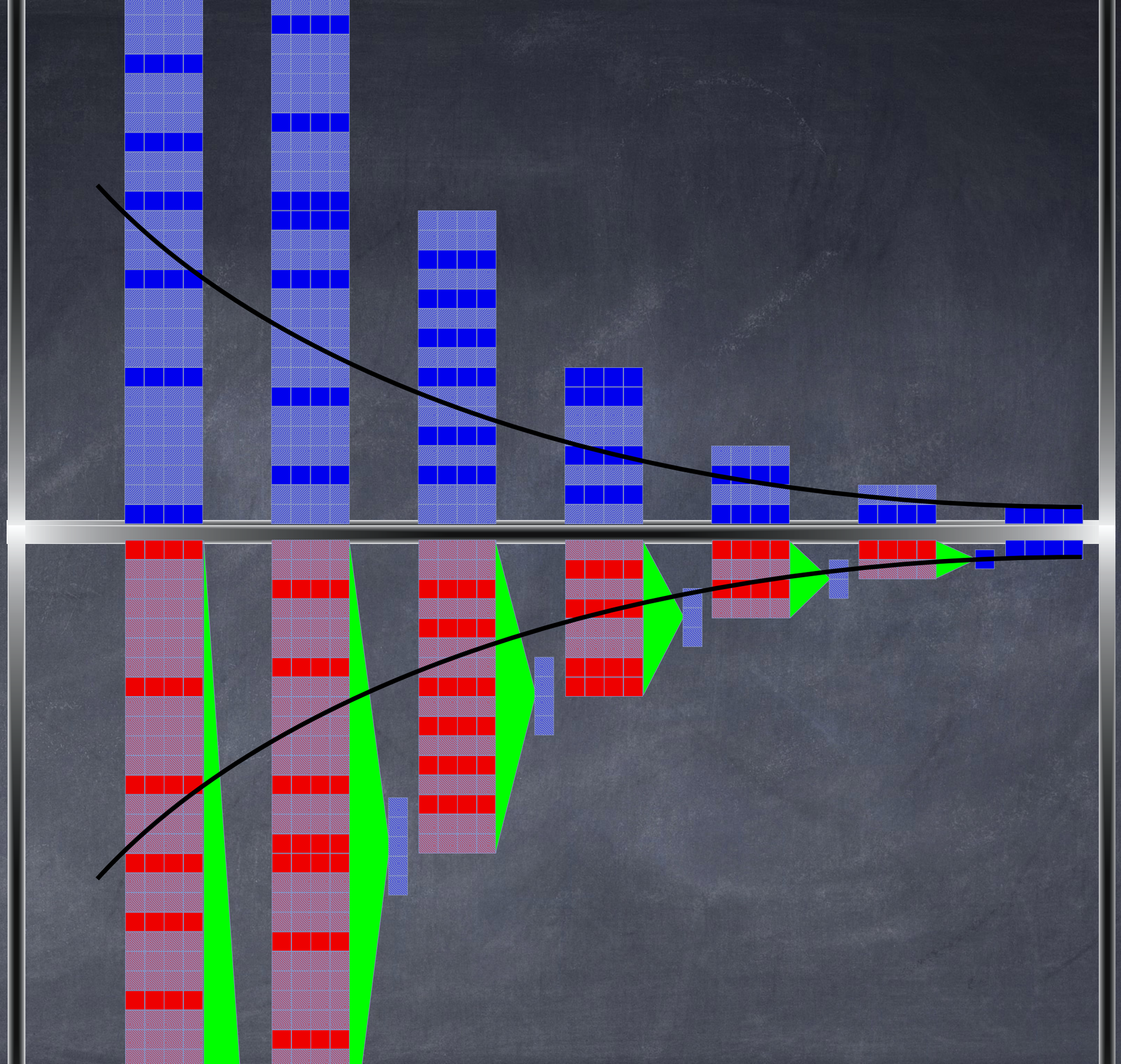


Truely Random Function



Pseudo-random Function Generator





Identification from PRFG

#6

pseudo-key #6

OK !

pseudo-key #6

Identification from PRFG

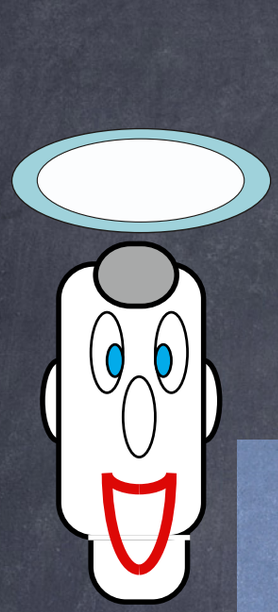
#6

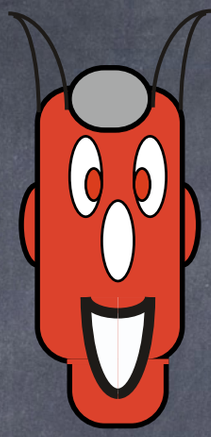
pseudo-key #6

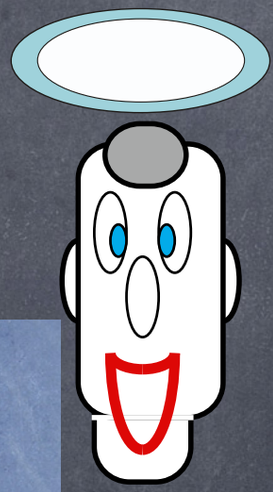
fail !

pseudo-key #6

Complexity Theoretical Asymmetric Cryptography







.....

public key distribution

asymmetric encryption

asymmetric authentication

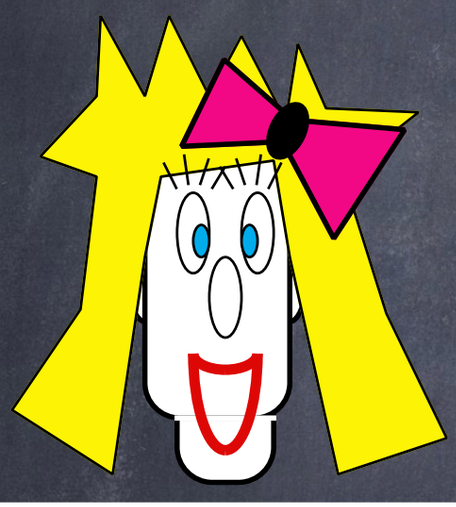
zero-knowledge identification

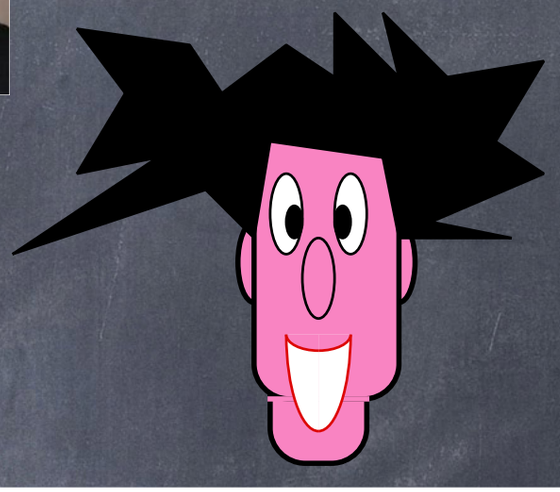
.....

Public Key Distribution

Public-Key Distribution

p



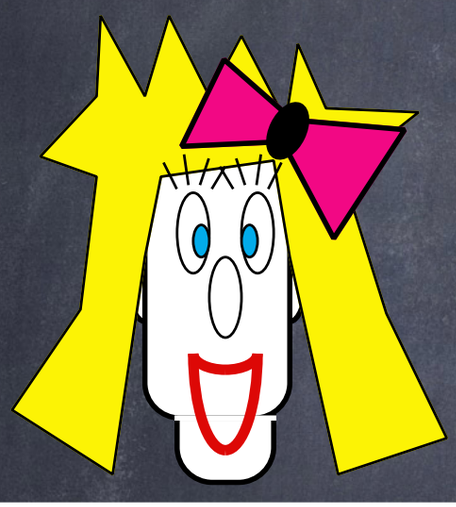


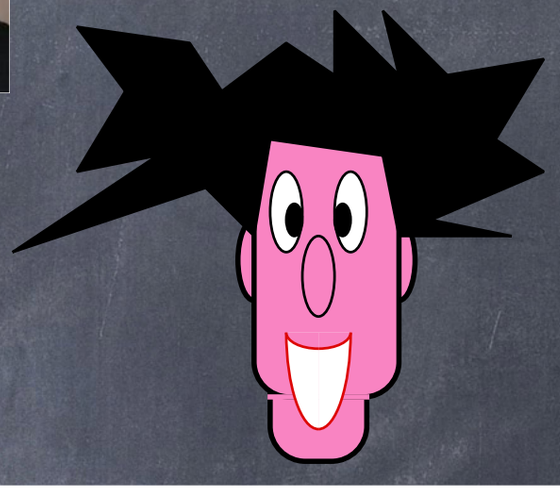
x:=f(p,a)

y:=f(p,b)

Public-Key Distribution

p





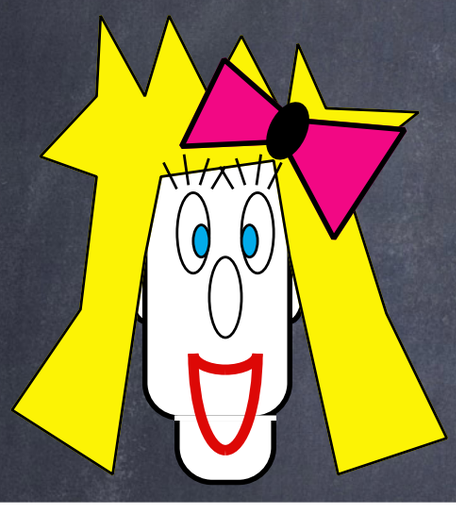
x:=f(p,a)

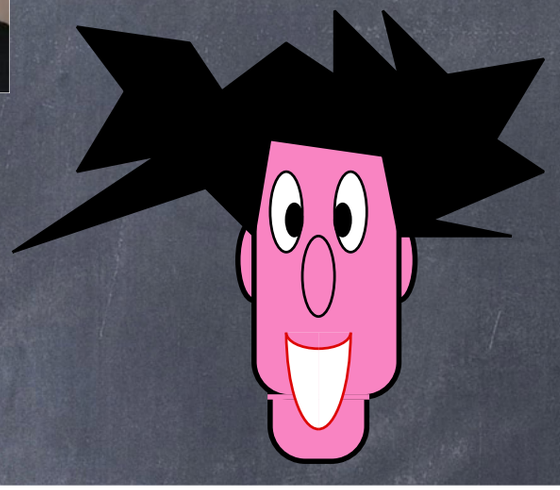
x

y:=f(p,b)

Public-Key Distribution

p





x:=f(p,a)

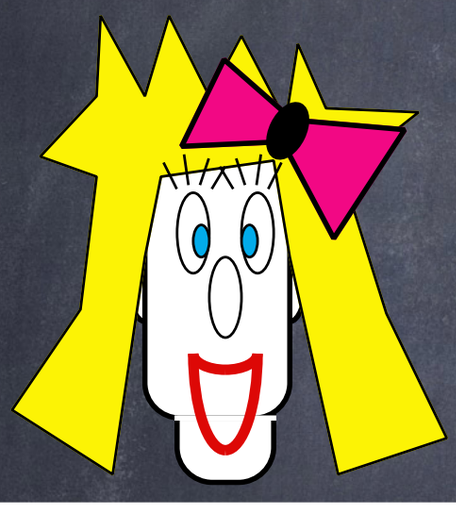
y:=f(p,b)

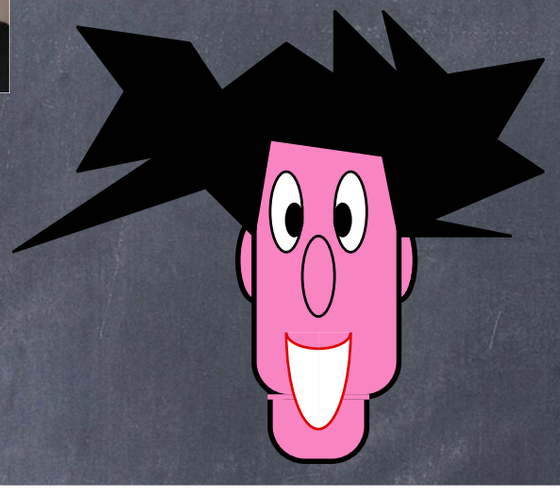
x

y

Public-Key Distribution

p





x:=f(p,a)

y:=f(p,b)

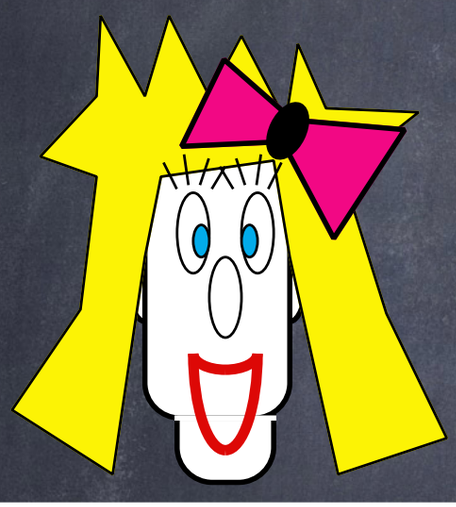
x

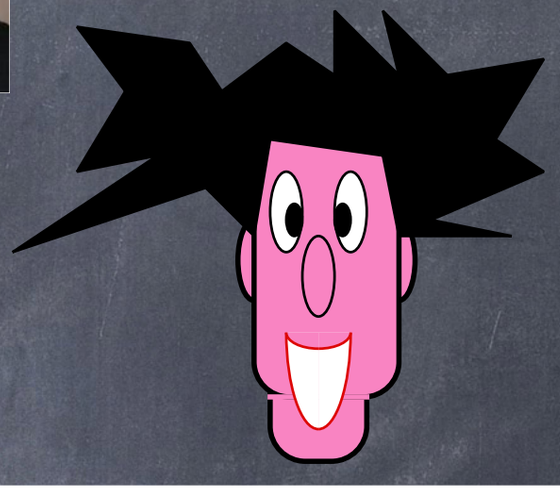
y

k:=f(x,b)

Public-Key Distribution

p





x:=f(p,a)

y:=f(p,b)

x

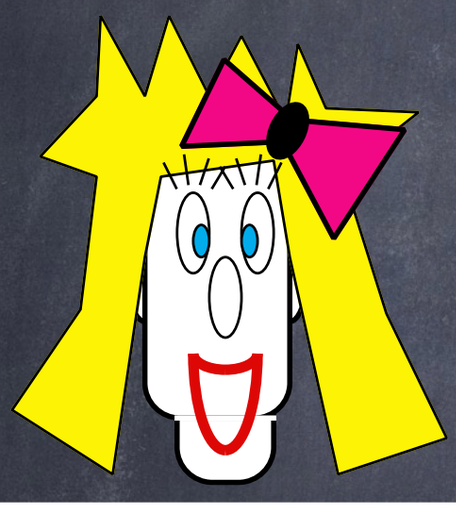
y

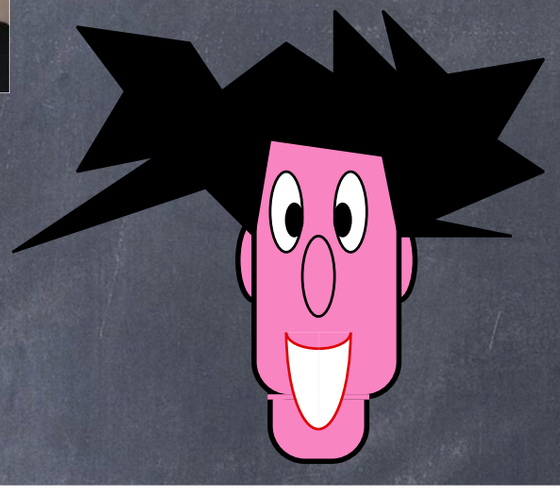
k:=f(y,a)

k:=f(x,b)

Public-Key Distribution

p





x:=f(p,a)

y:=f(p,b)

x

y

k:=f(y,a)

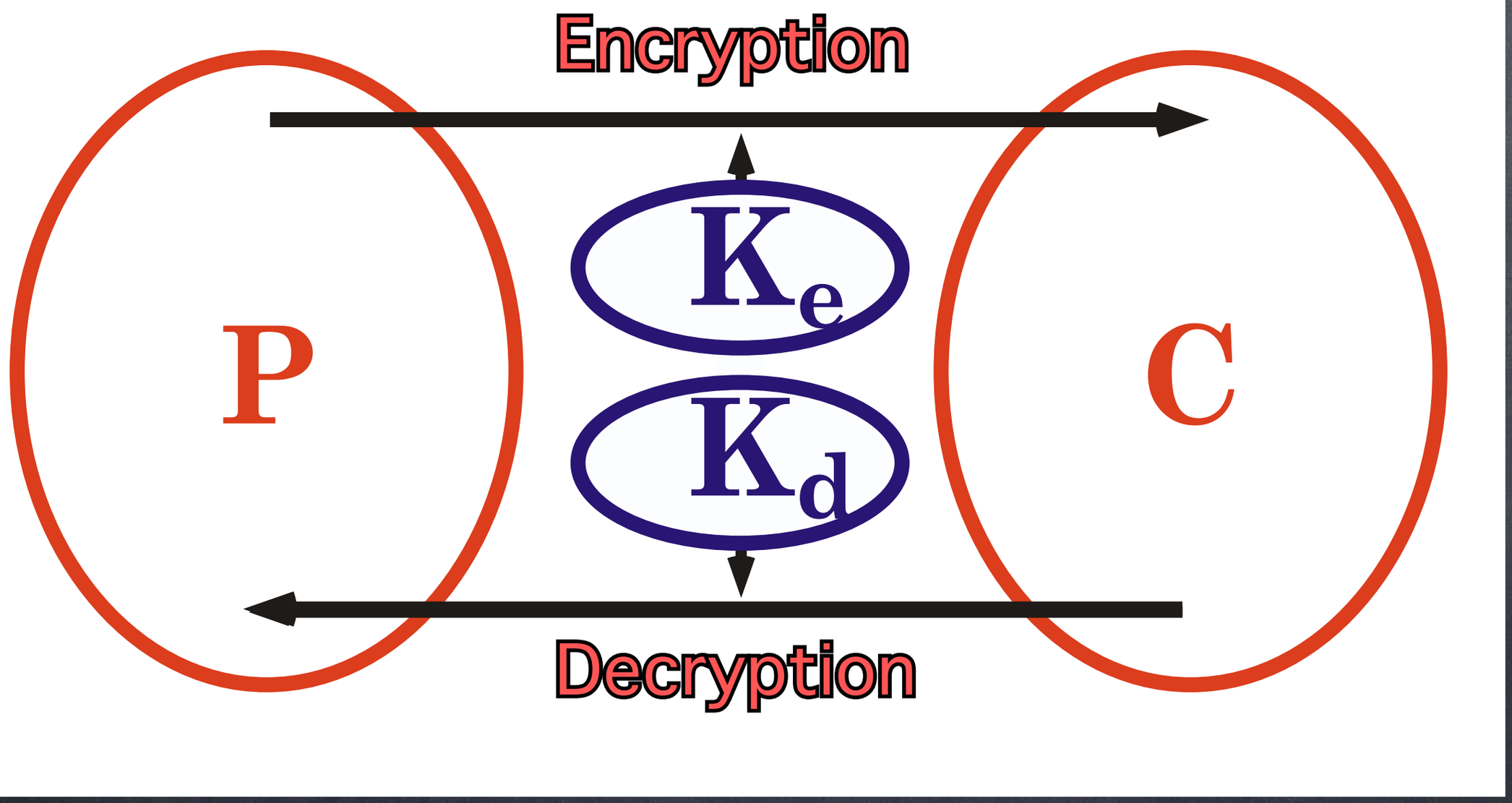
k:=f(x,b)

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

Public Key Encryption

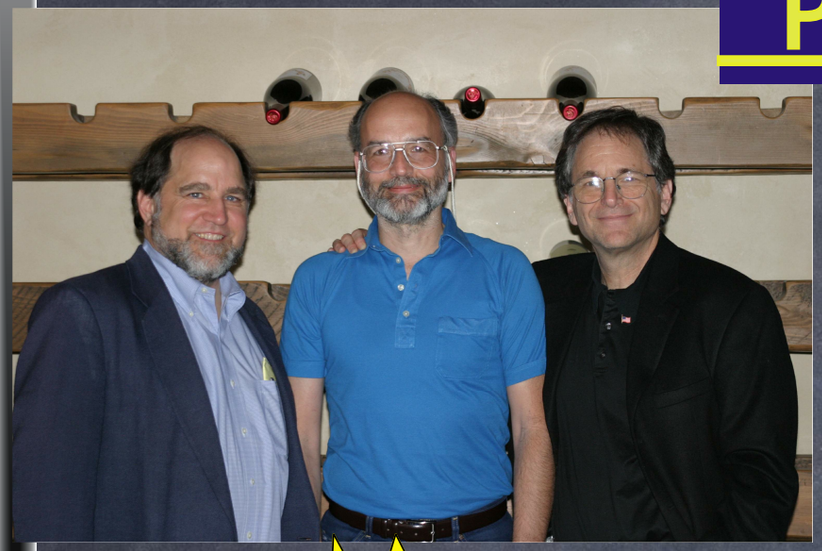
Asymmetric Encryption

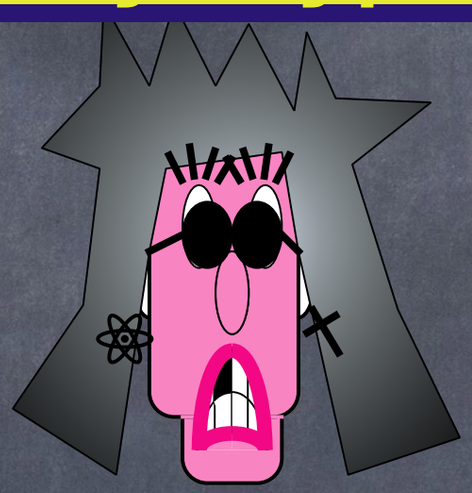
(Public-Key Cryptography)

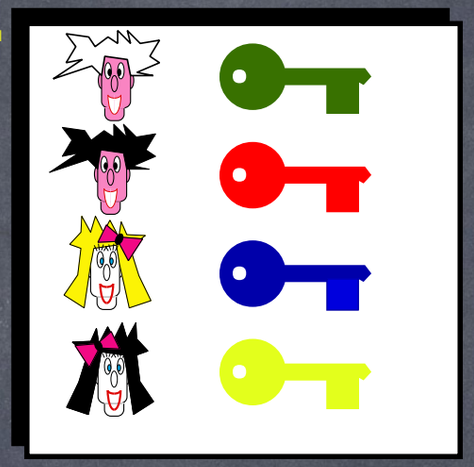


Complexity Theoretical Security

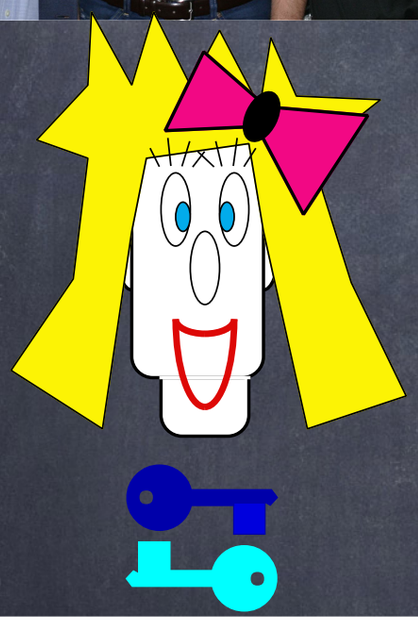
Public-Key Cryptography

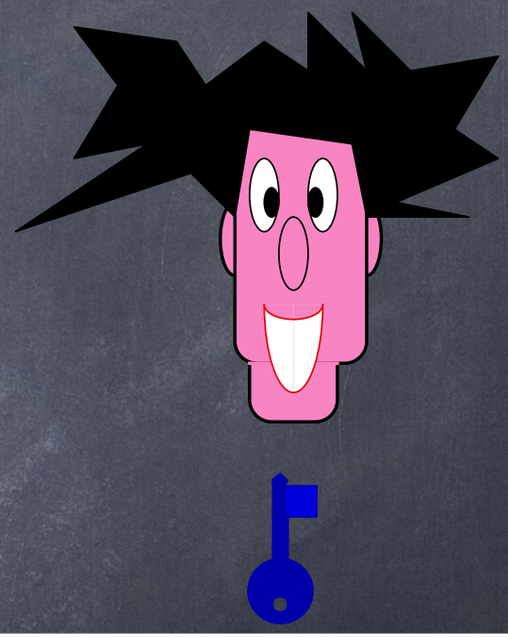




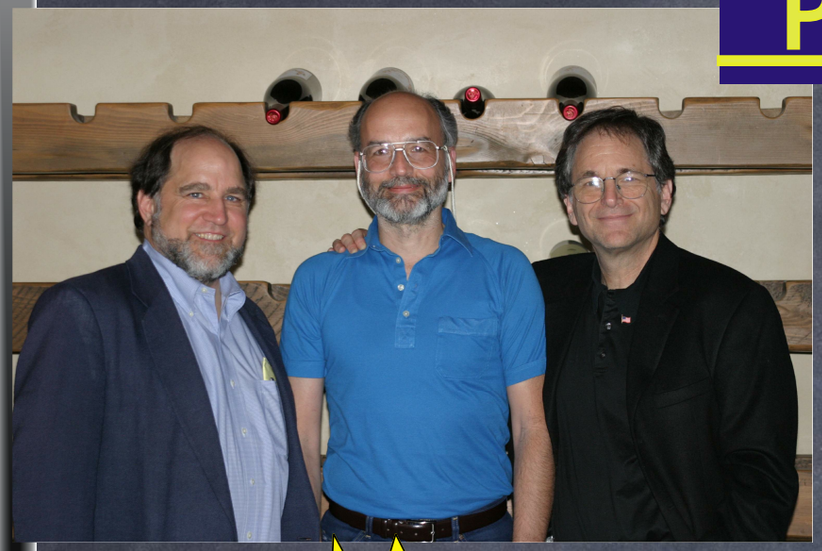


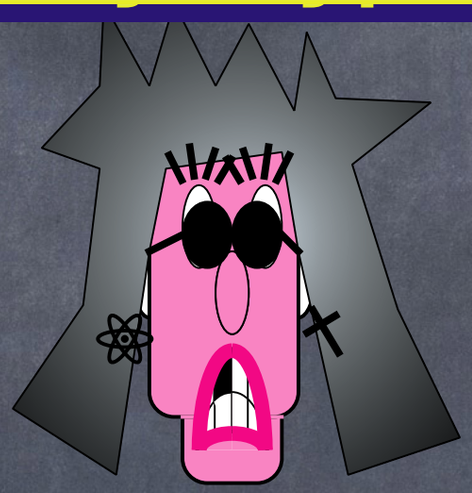
8RdewtU5qkLa$es!T9@

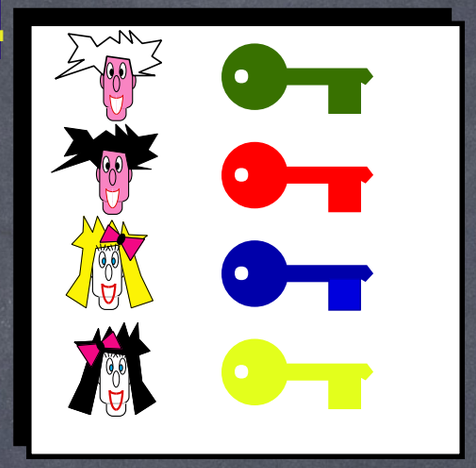


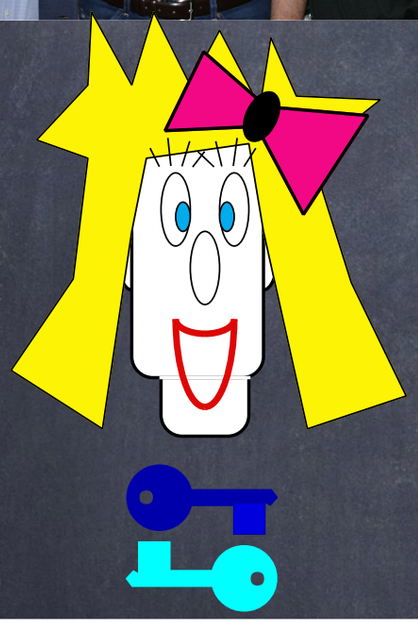


Public-Key Cryptography

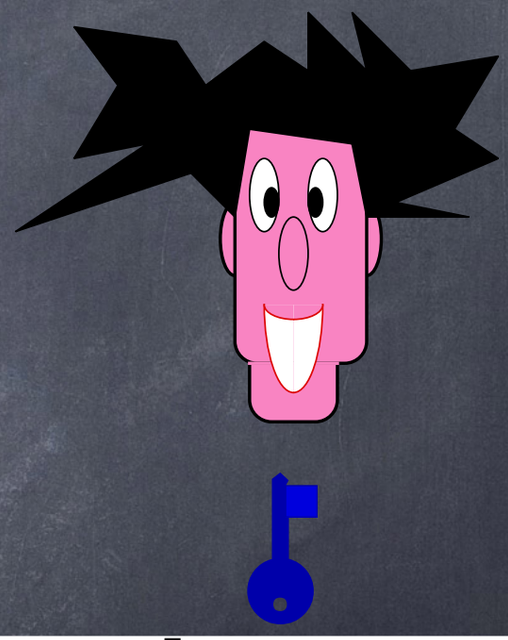




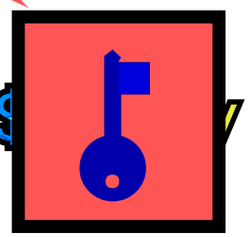




8RdewtU5qkLa$es!T9@

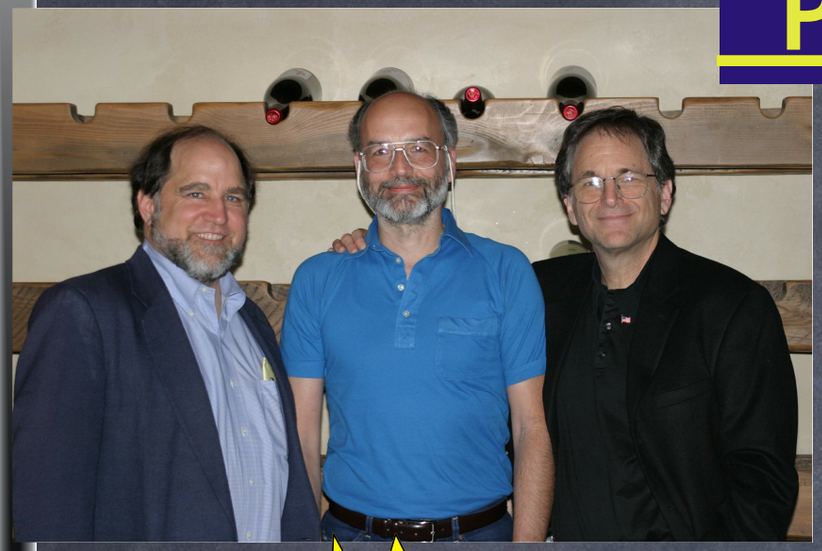


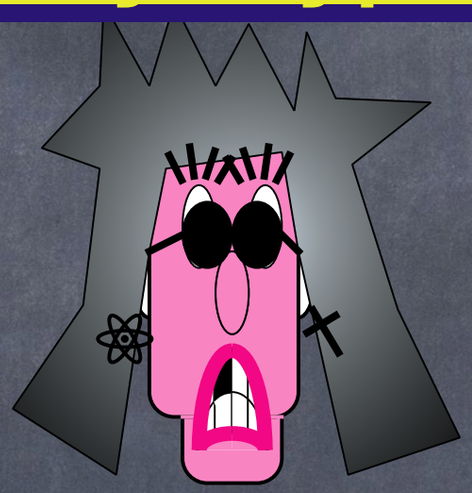
Encryption

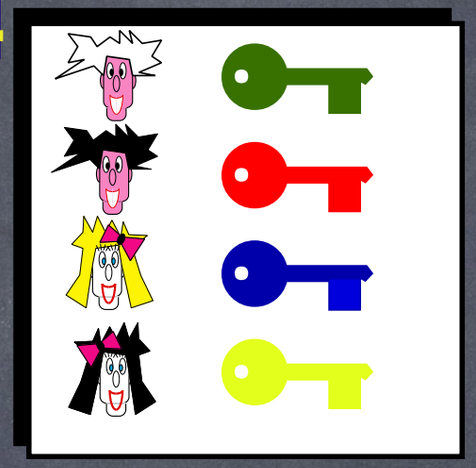


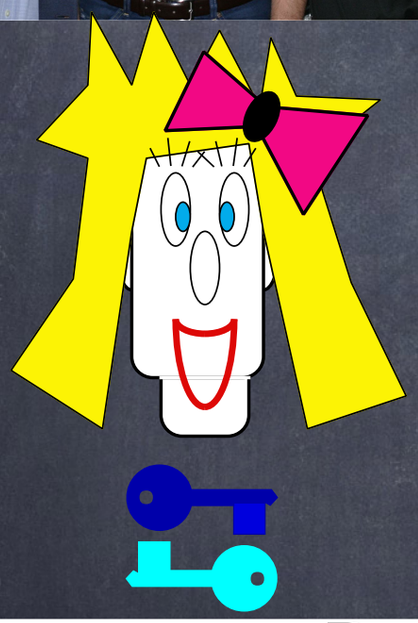
8RdewtU5qkLa$ [illegible] me ?

Public-Key Cryptography

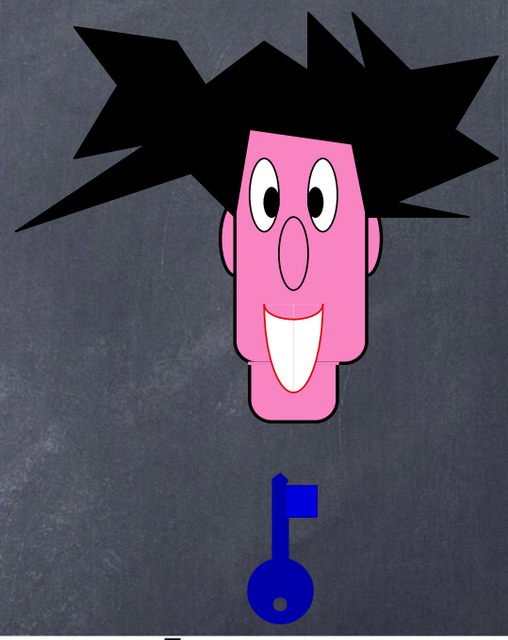








8RdewtU5qkLa$es!T9@



Decryption

Will you marry m es!T9@

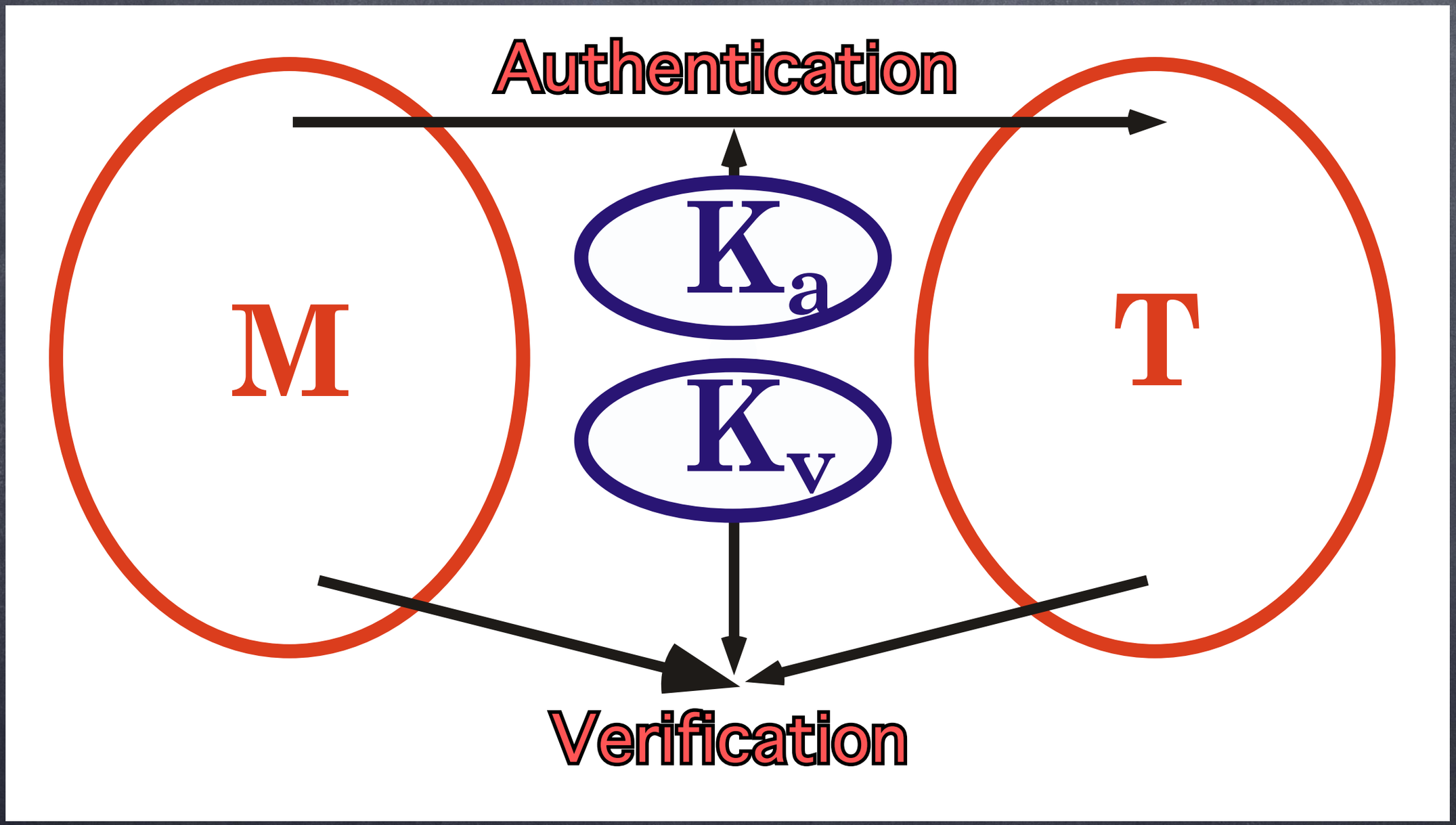
Encryption

8RdewtU5qkLa$ y me ?

Digital Signatures

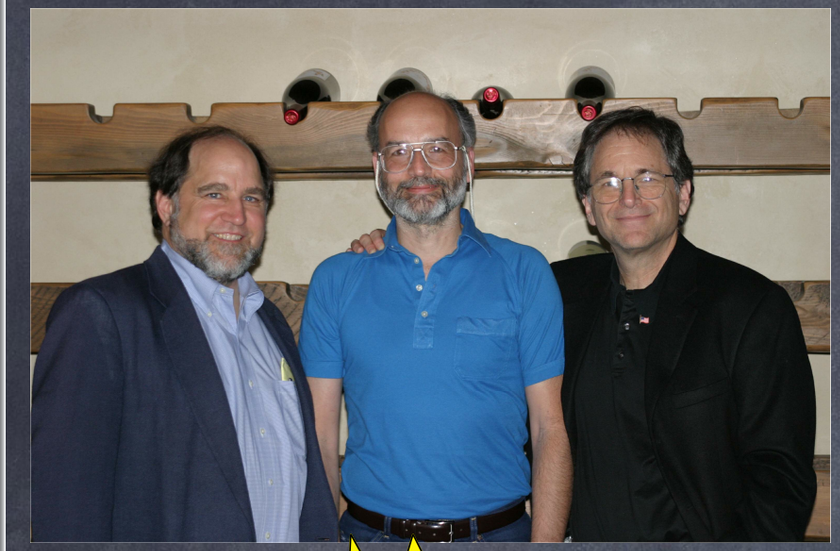
Asymmetric Authentication

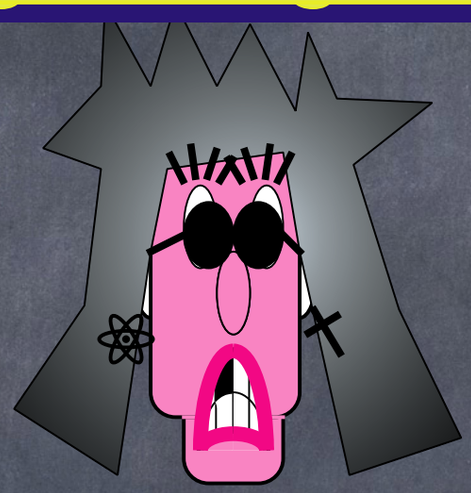
(Digital Signature Scheme)

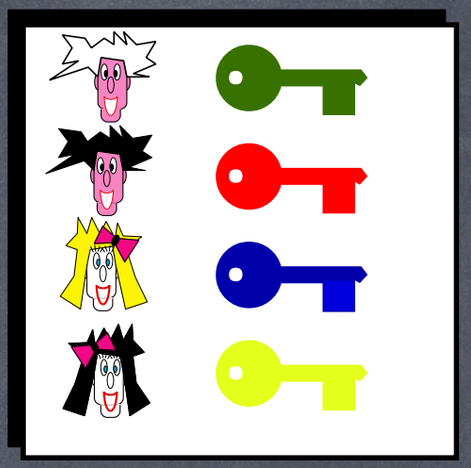


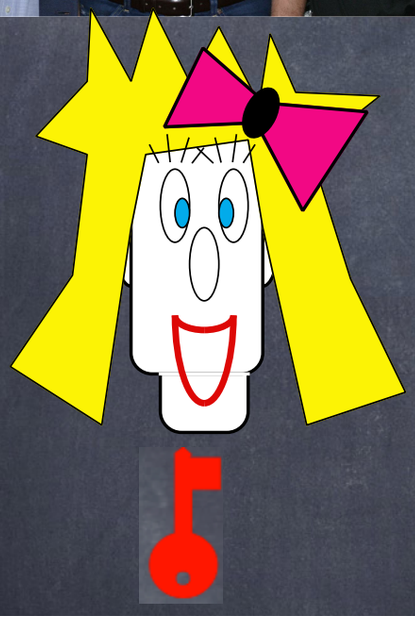
Complexity Theoretical Security

Digital Signature

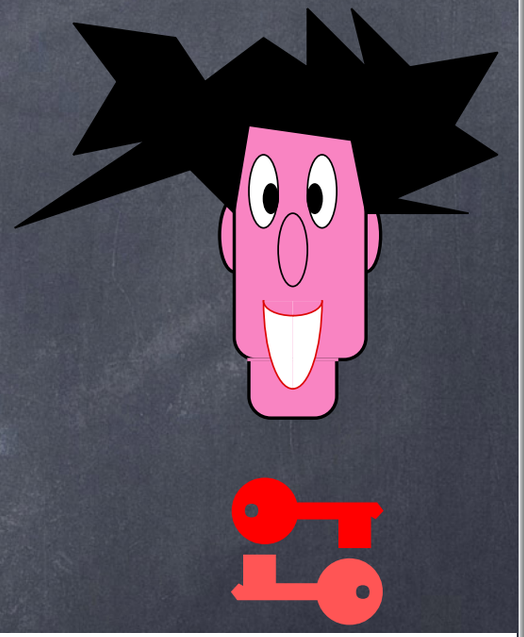




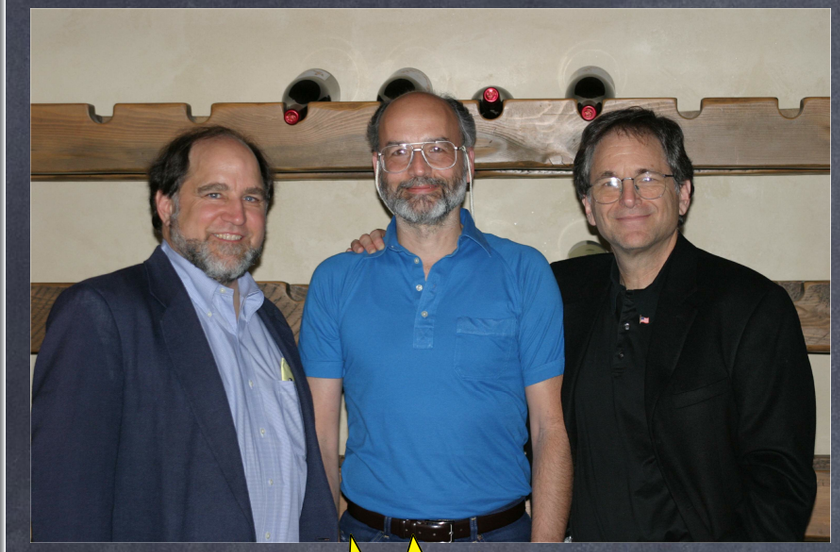


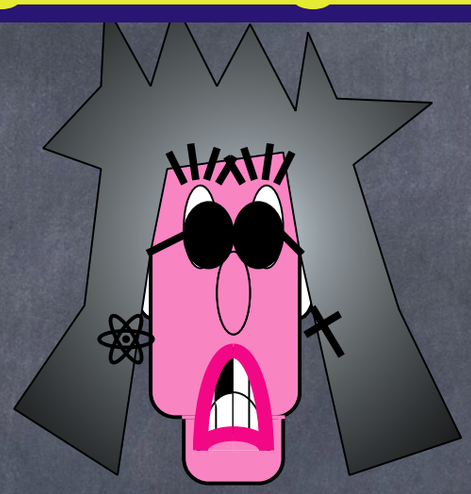


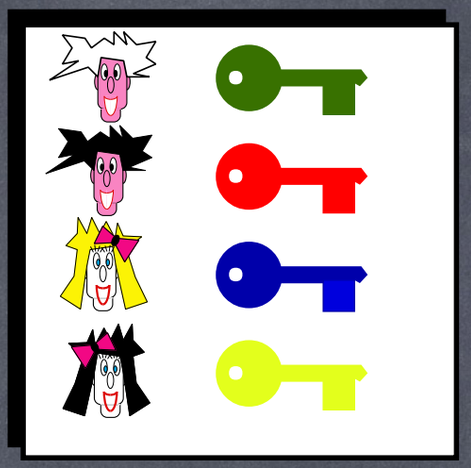
8RdewtU5qkLa$es!T9@
Will you marry me ?

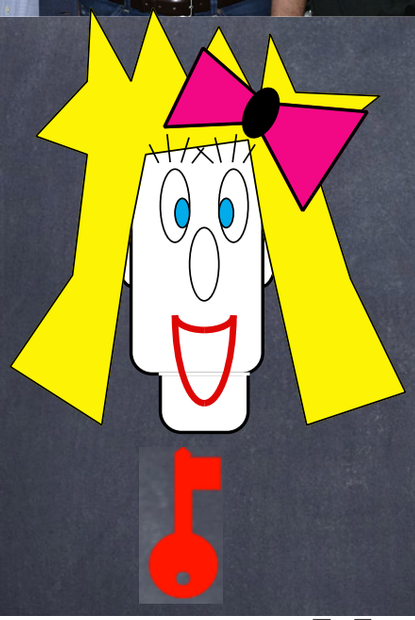


Digital Signature

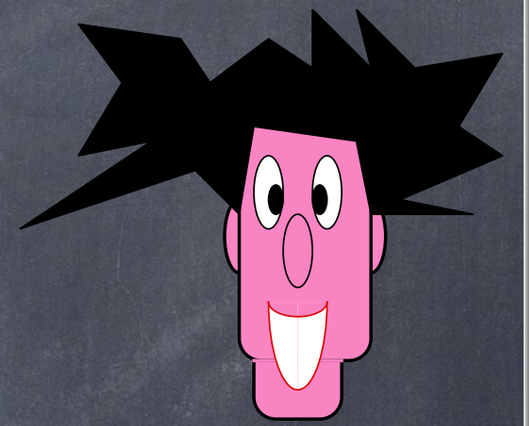








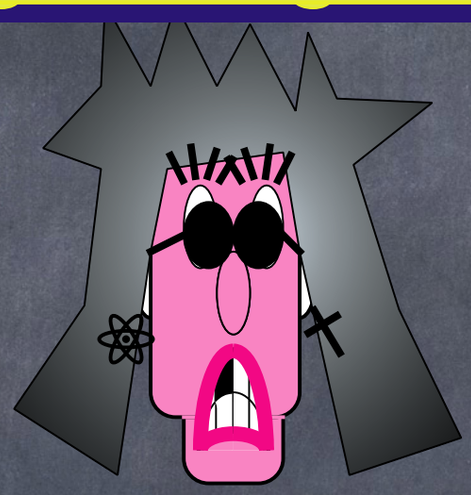
8RdewtU5qkLa$es!T9@
Will you marry me ?

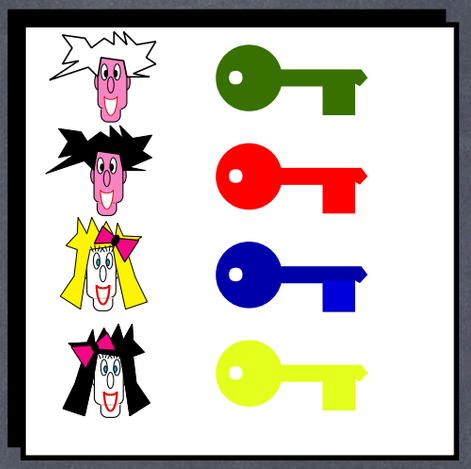


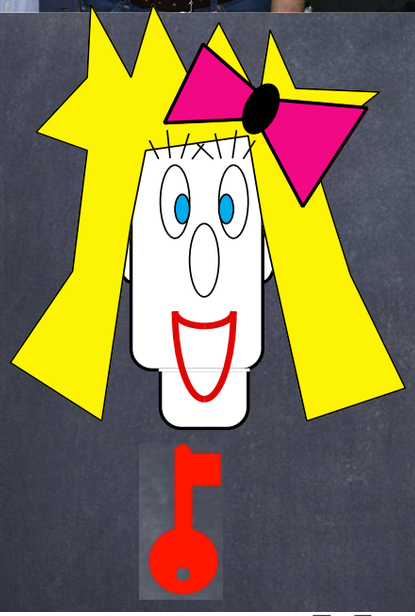
Authentication

8RdewtU5qkLa$ me ?

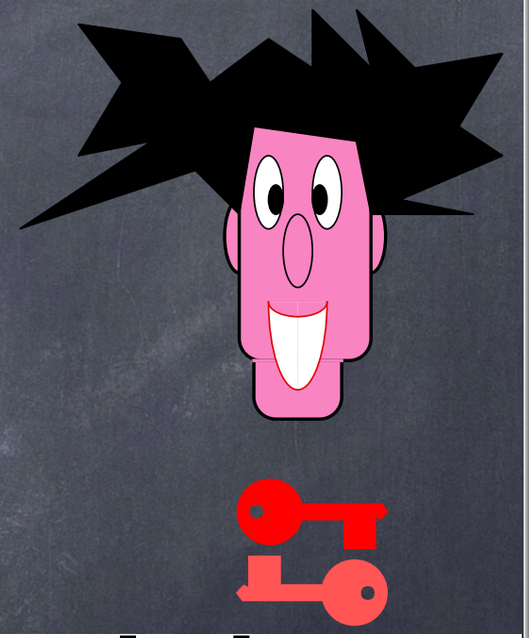
Digital Signature







8RdewtU5qkLa$es!T9@
Will you marry me ?



Verification

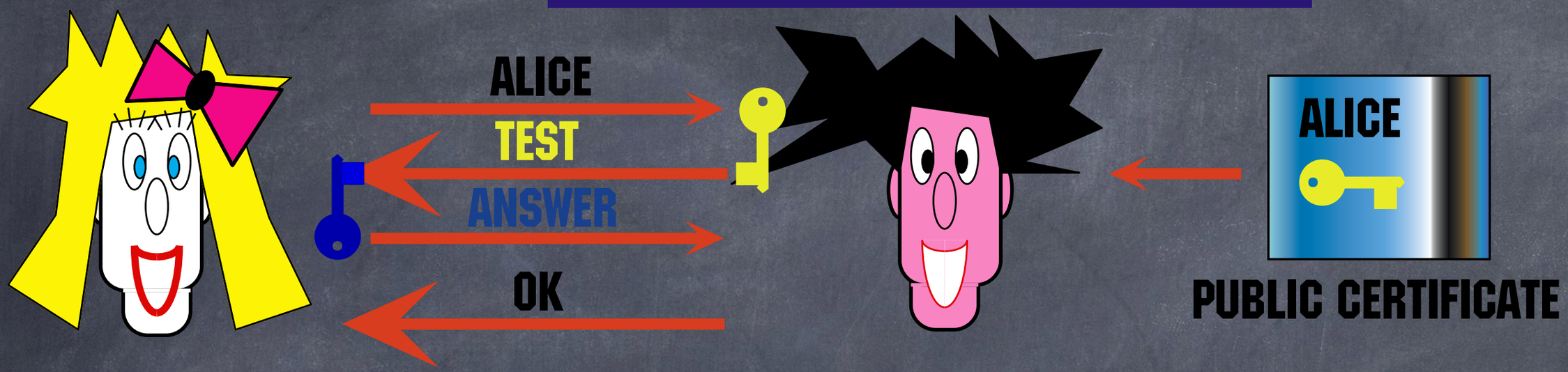
VALID  es!T9@
ry me ?

Authentication

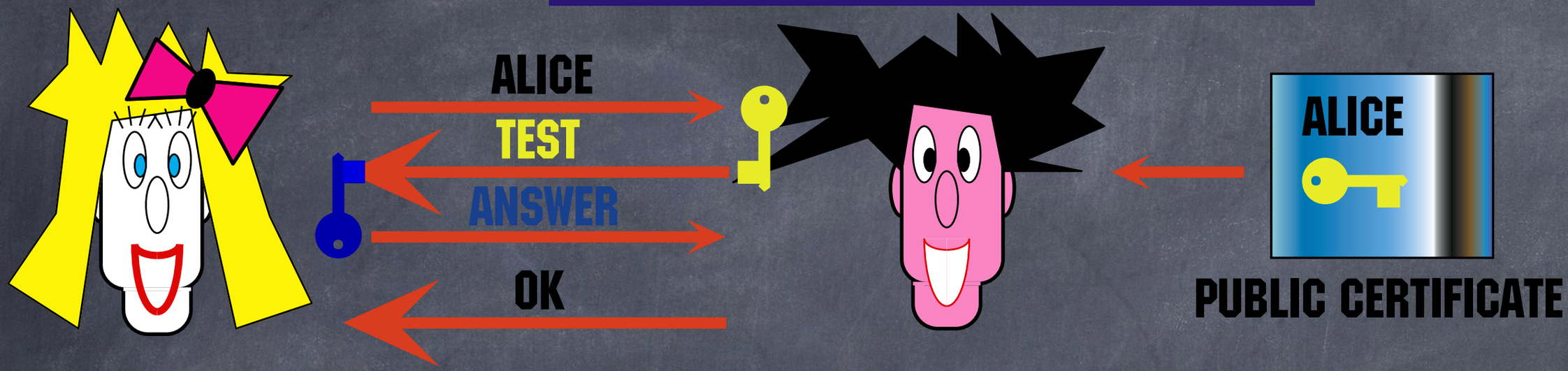
8RdewtU5qkLa$  y me ?

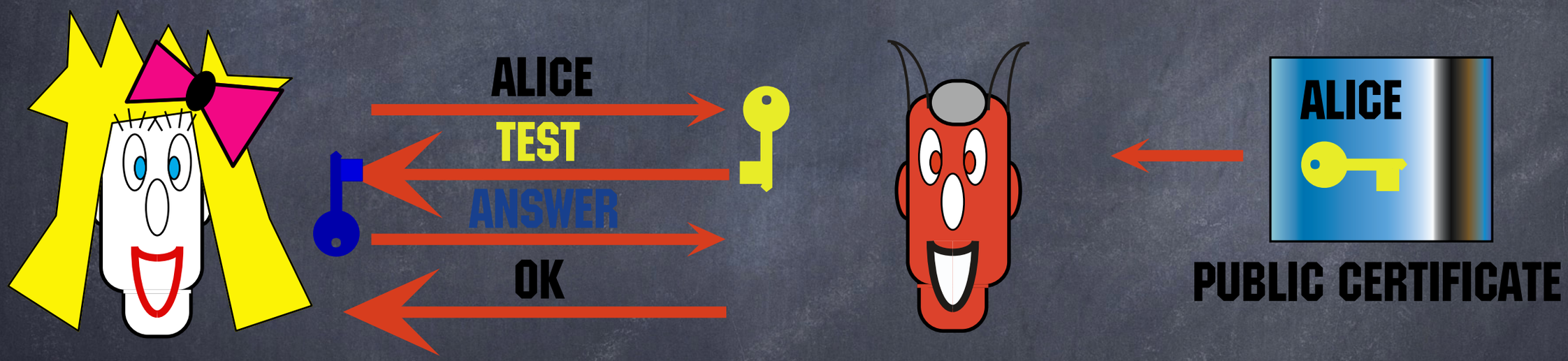
Zero-Knowledge Identification

Off-line Identification

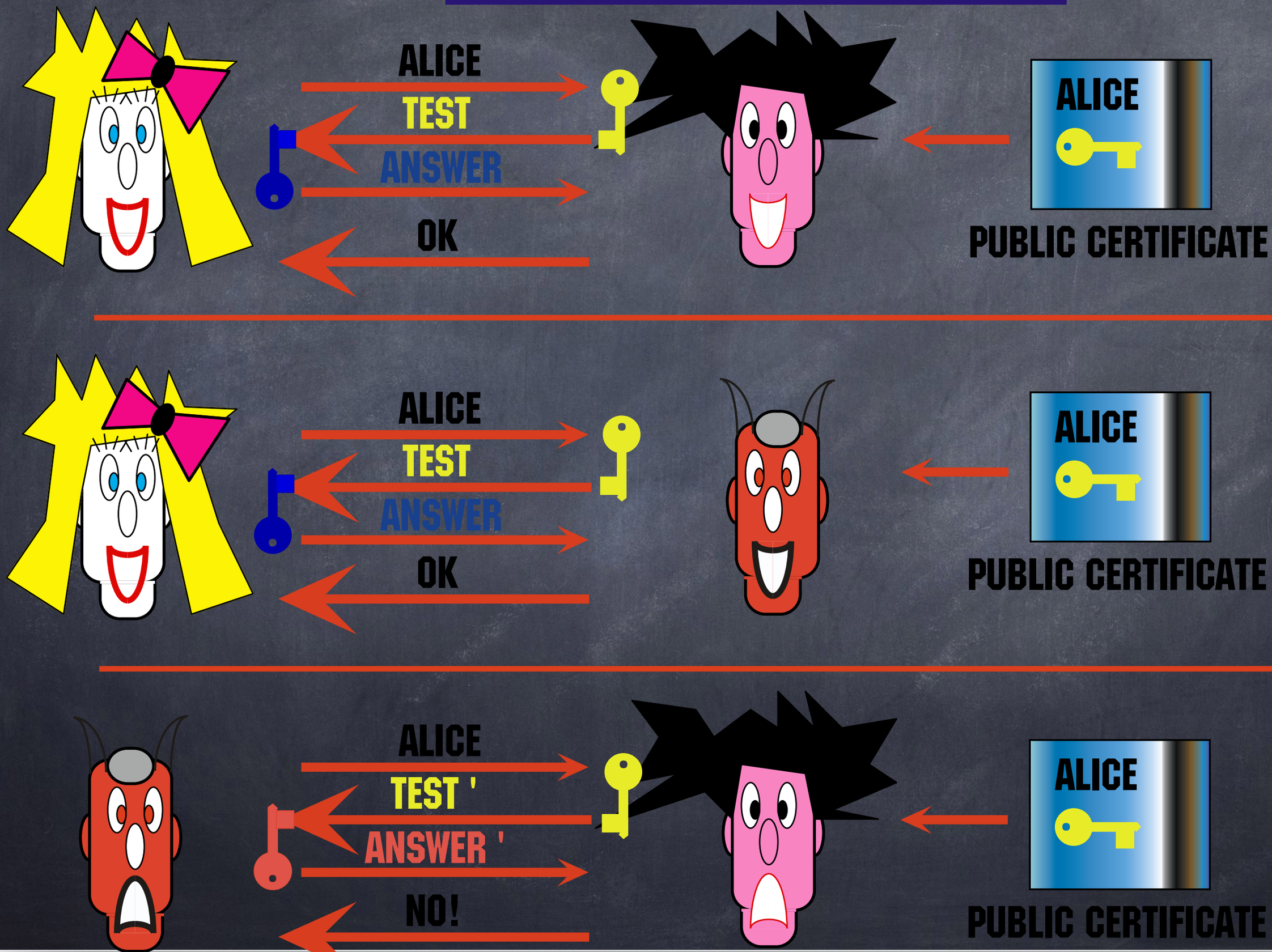


Off-line Identification

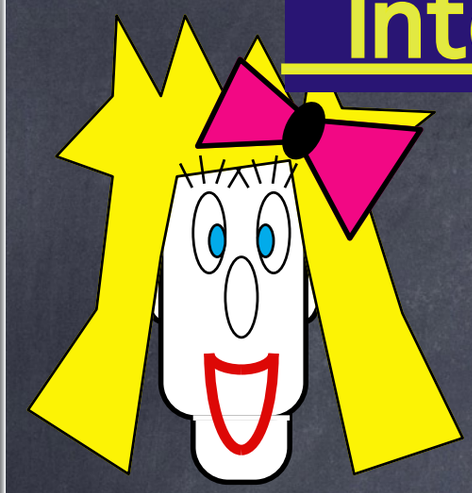




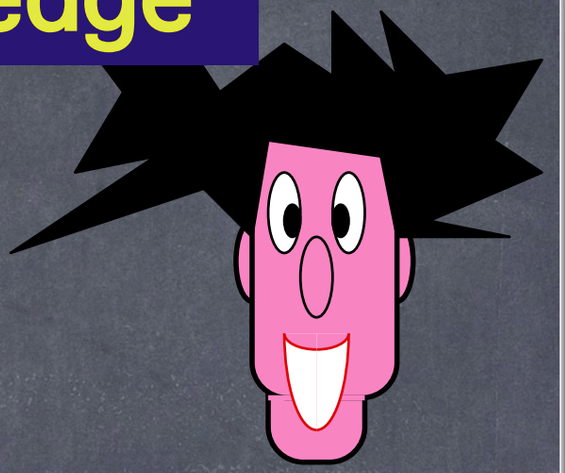
Off-line Identification



Interactive Proofs and Zero-Knowledge



$x \in L$

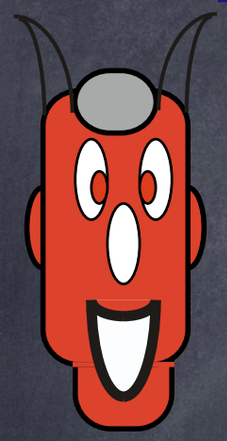


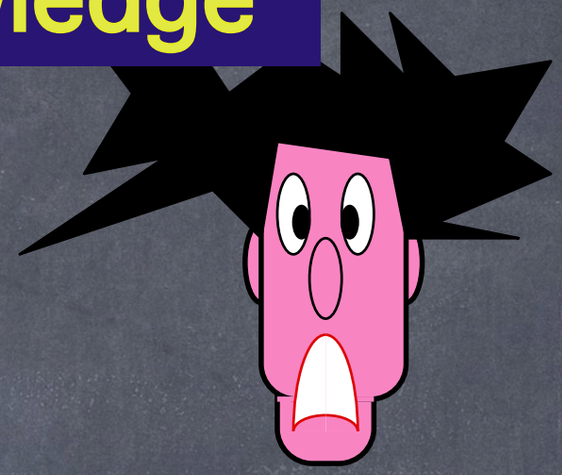
YES !

$$\forall x \in L \; \Pr([A,B](x)=\text{YES}) \approx 1$$

Interactive Proofs and Zero-Knowledge

$x \notin L$

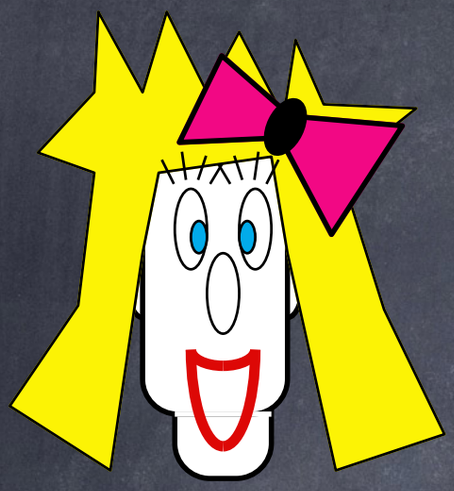




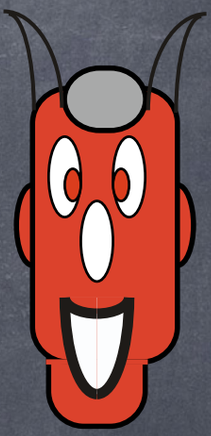
NO !

$$\forall x \notin L \; \forall D \; \Pr(\; [D,B](x)=\text{YES} \;) \approx 0$$

Interactive Proofs and Zero-Knowledge

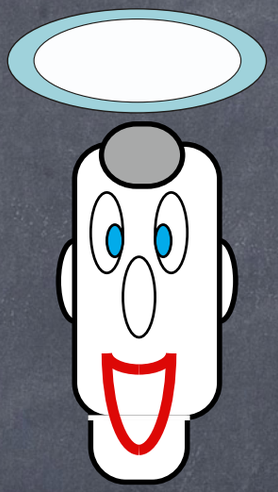


$x \in L$

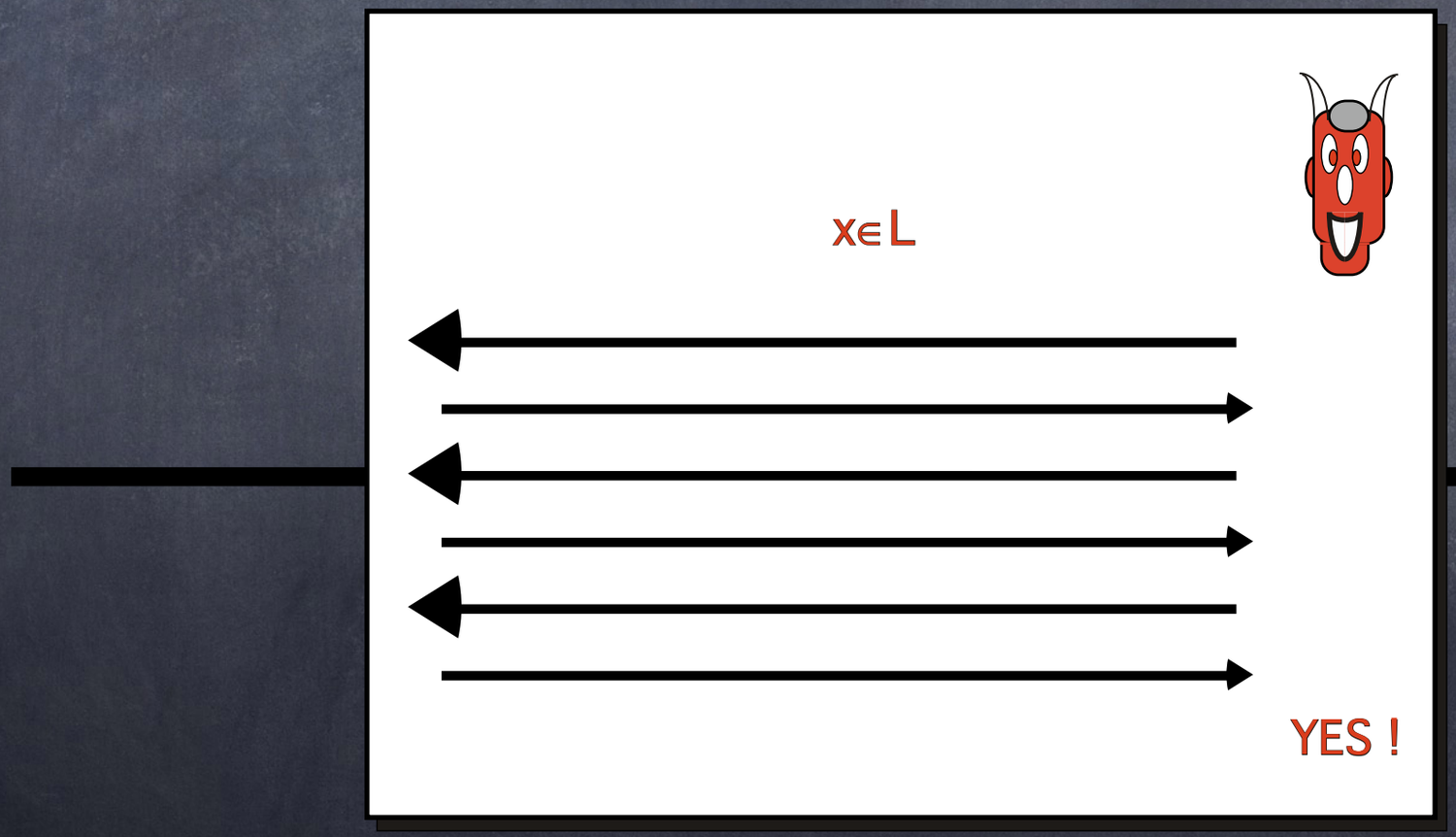


YES !

Interactive Proofs and NOT Zero-Knowledge

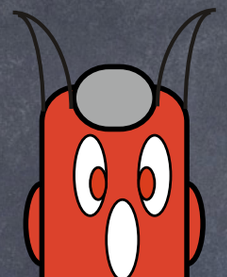


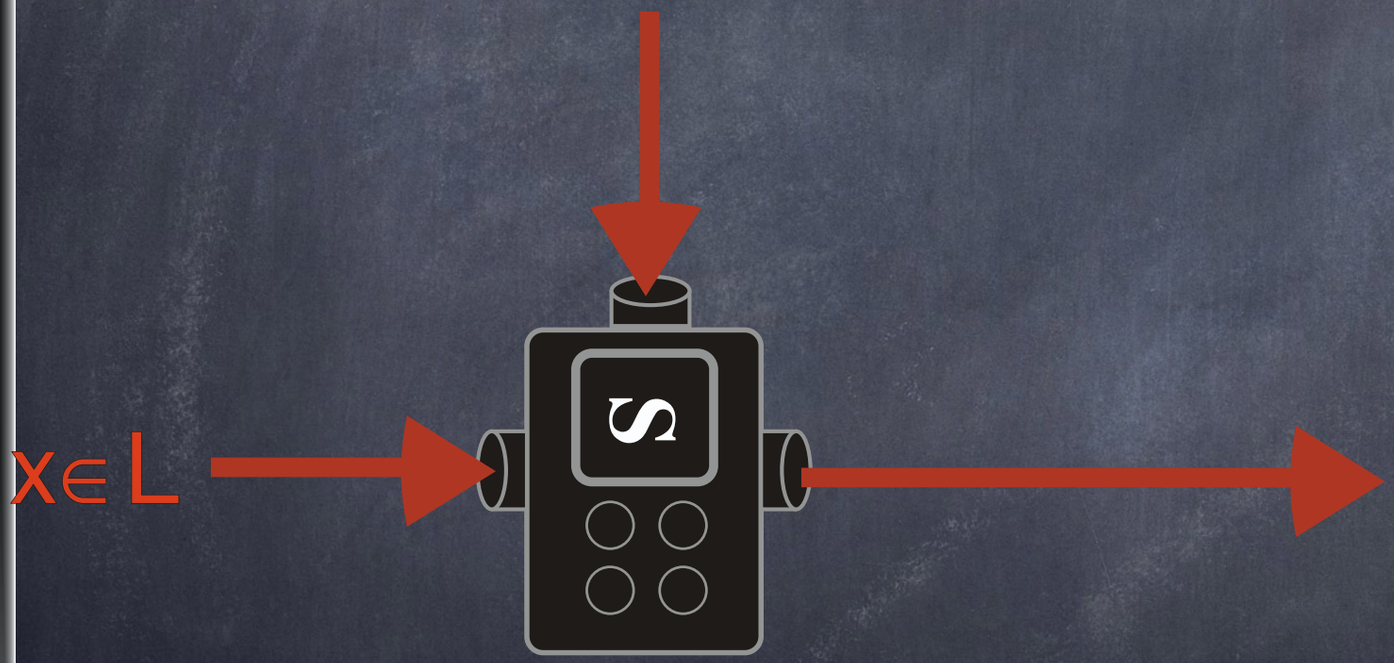
$x \in L$

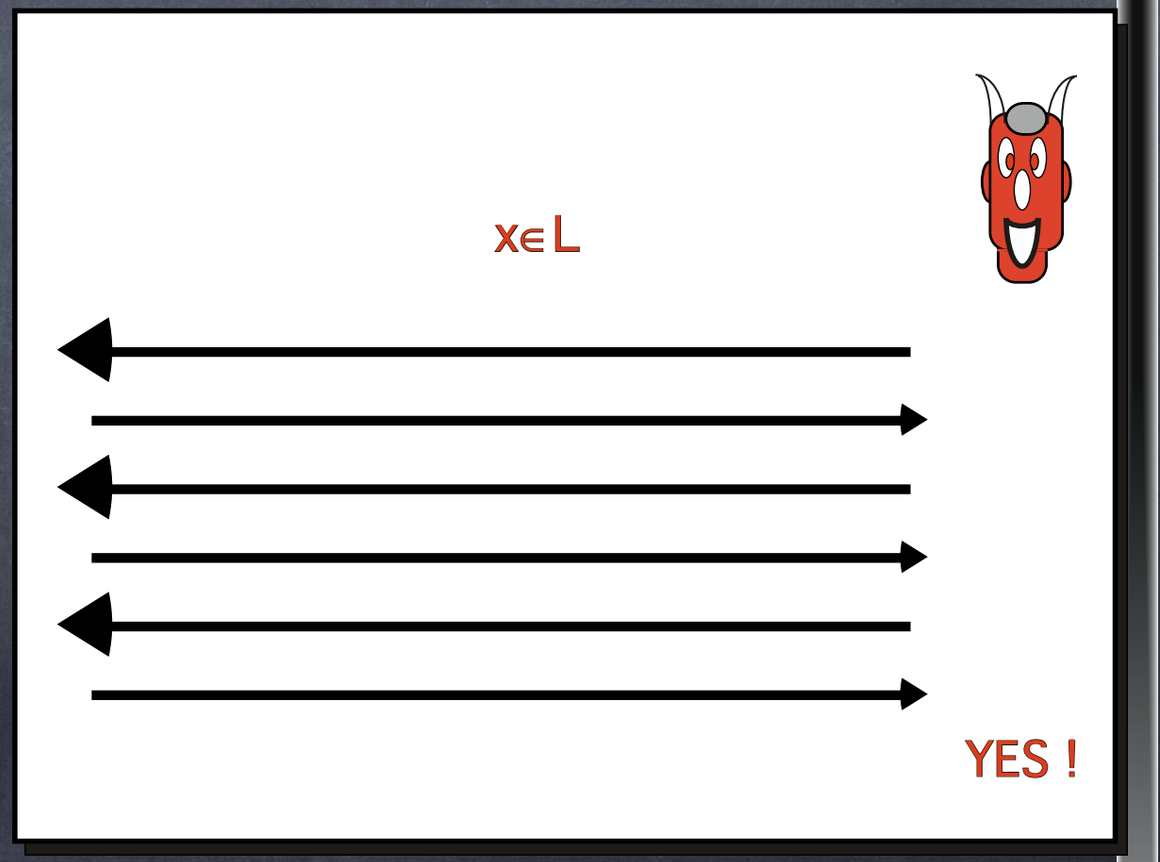


WOW !

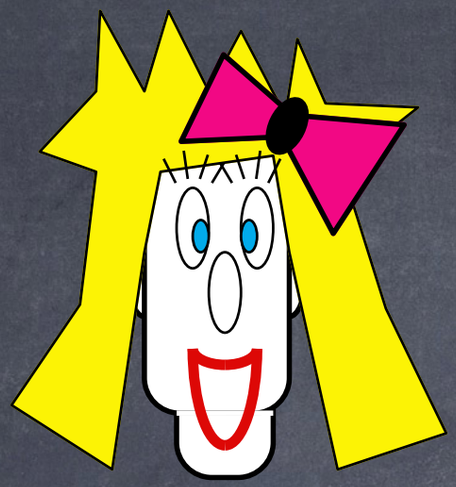
Zero-Knowledge with Simulator

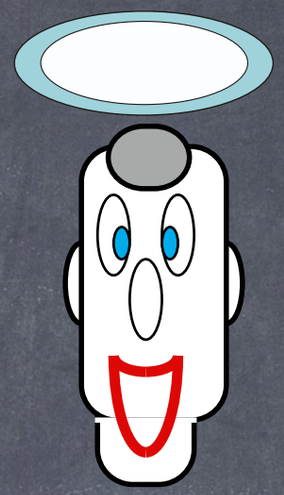




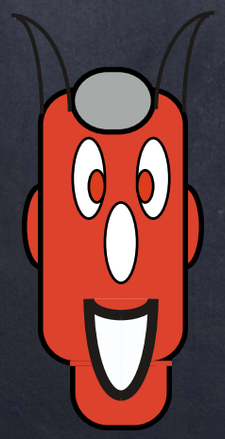


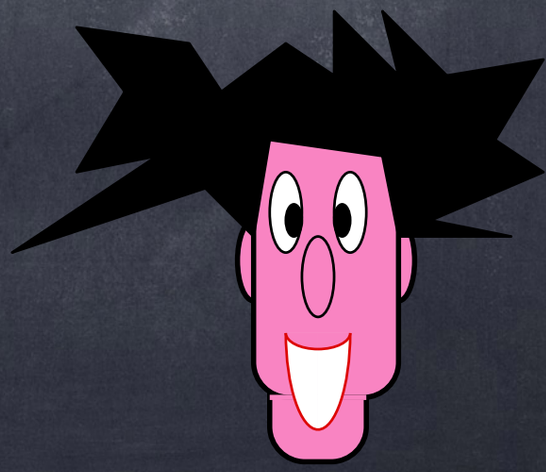
$$\forall_{eff} D \; \exists_{eff} S_D \; \forall x \in L \; view_D[A,D](x) = S_D(x)$$





CIAO !





COMP 102A, Lecture 16

Introduction to Cryptography II

COMP 102A, Lecture 16