COMP-199

Introduction to Cryptography

Lecture 02

Claude Crépeau

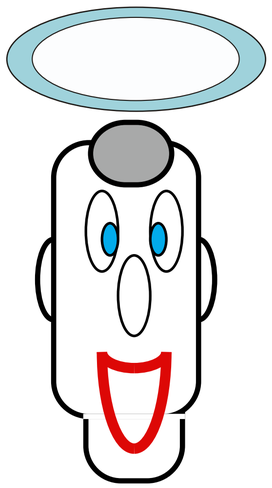
School of Computer Science
McGill University

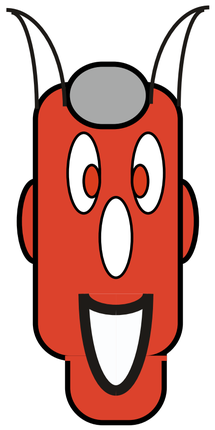
Complexity

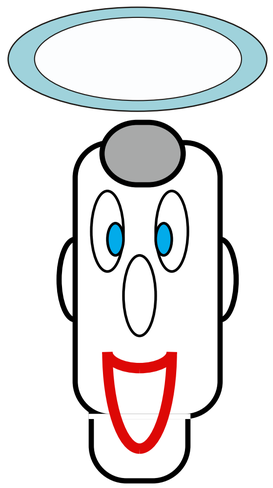
Theoretical

Cryptography

Complexity Theoretical Symmetric Cryptography







. . . . .

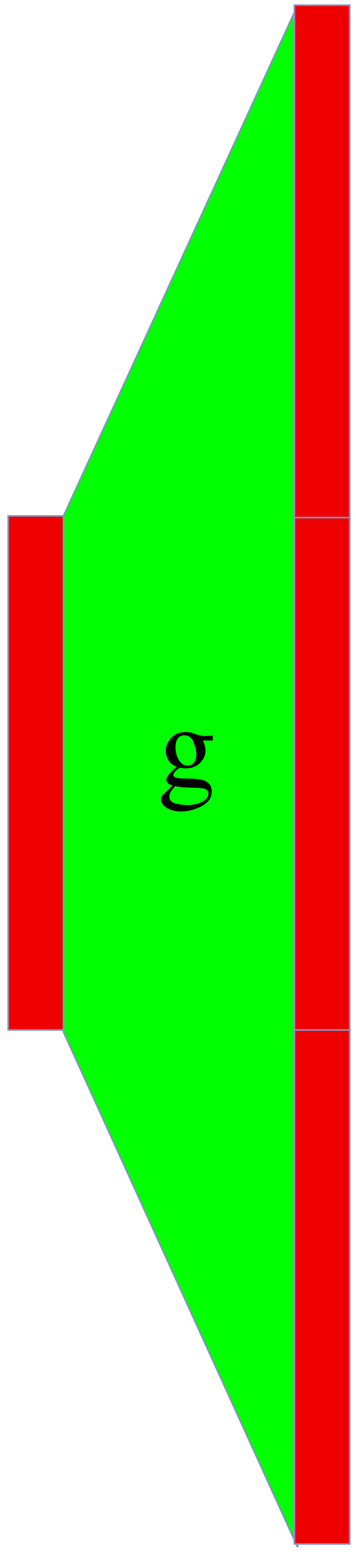
encryption

authentication

identification

. . . . .

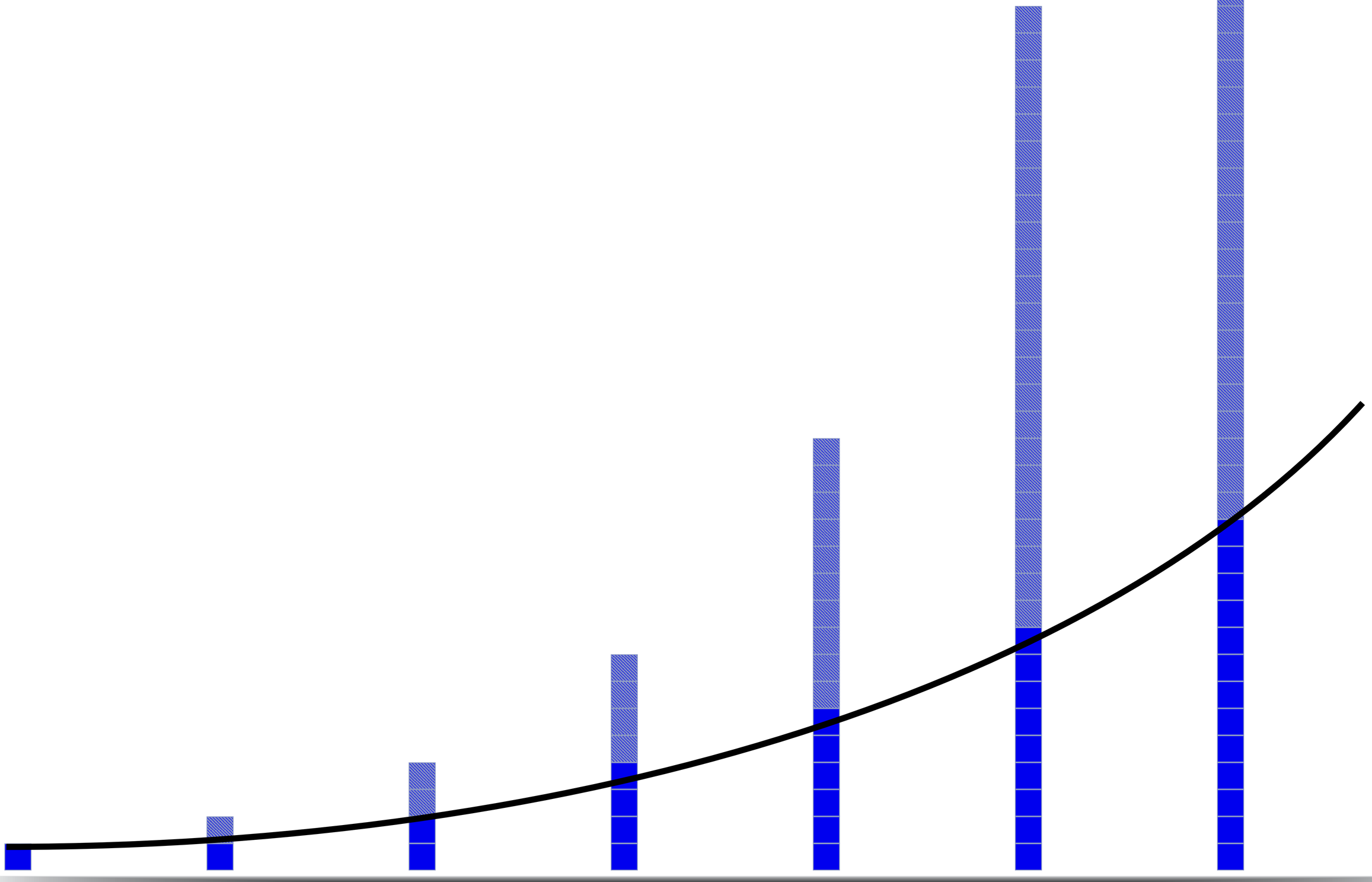
pseudo-random bit generator

RANDOM x 

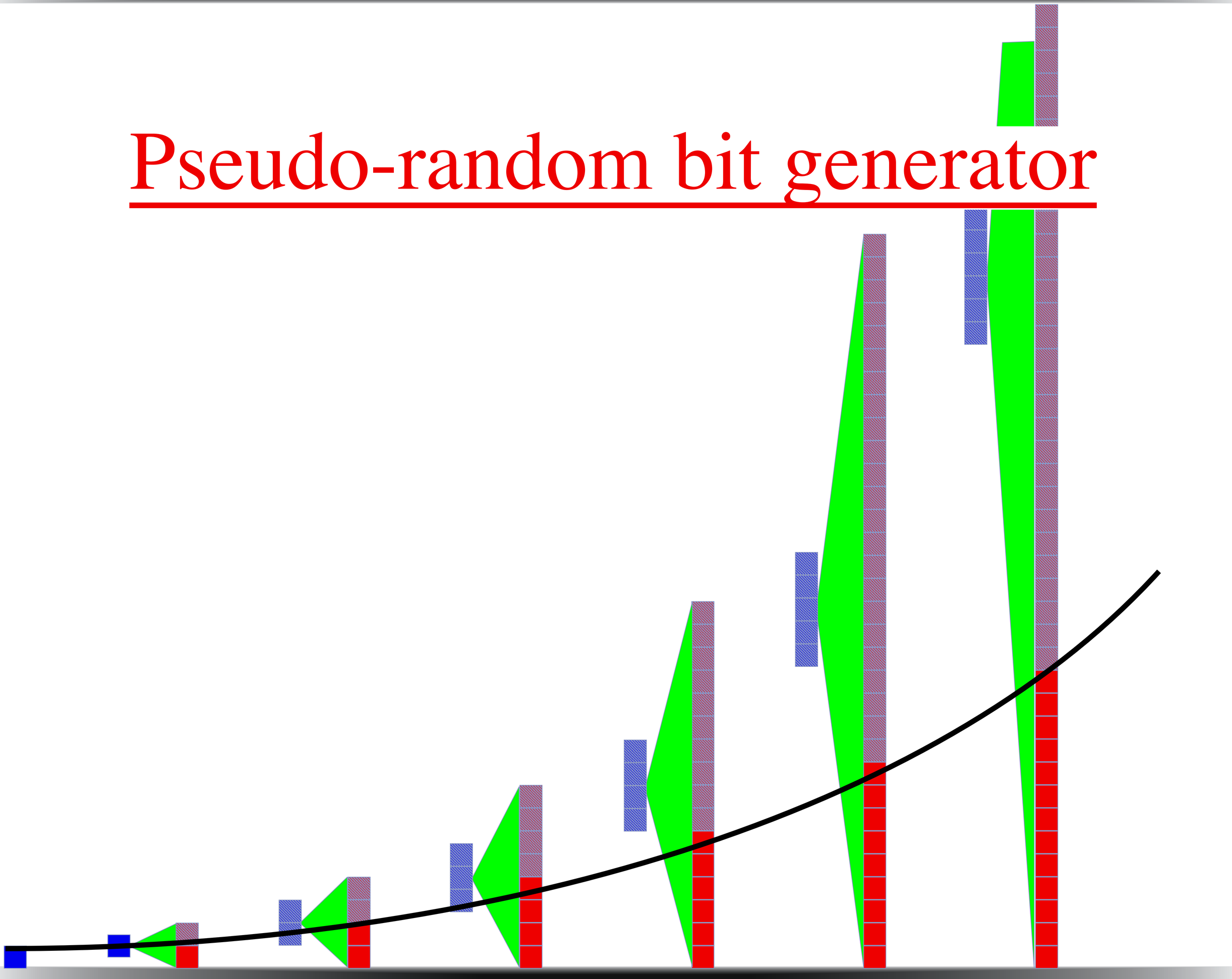
g(x)

SEEMS RANDOM

Truely random bits

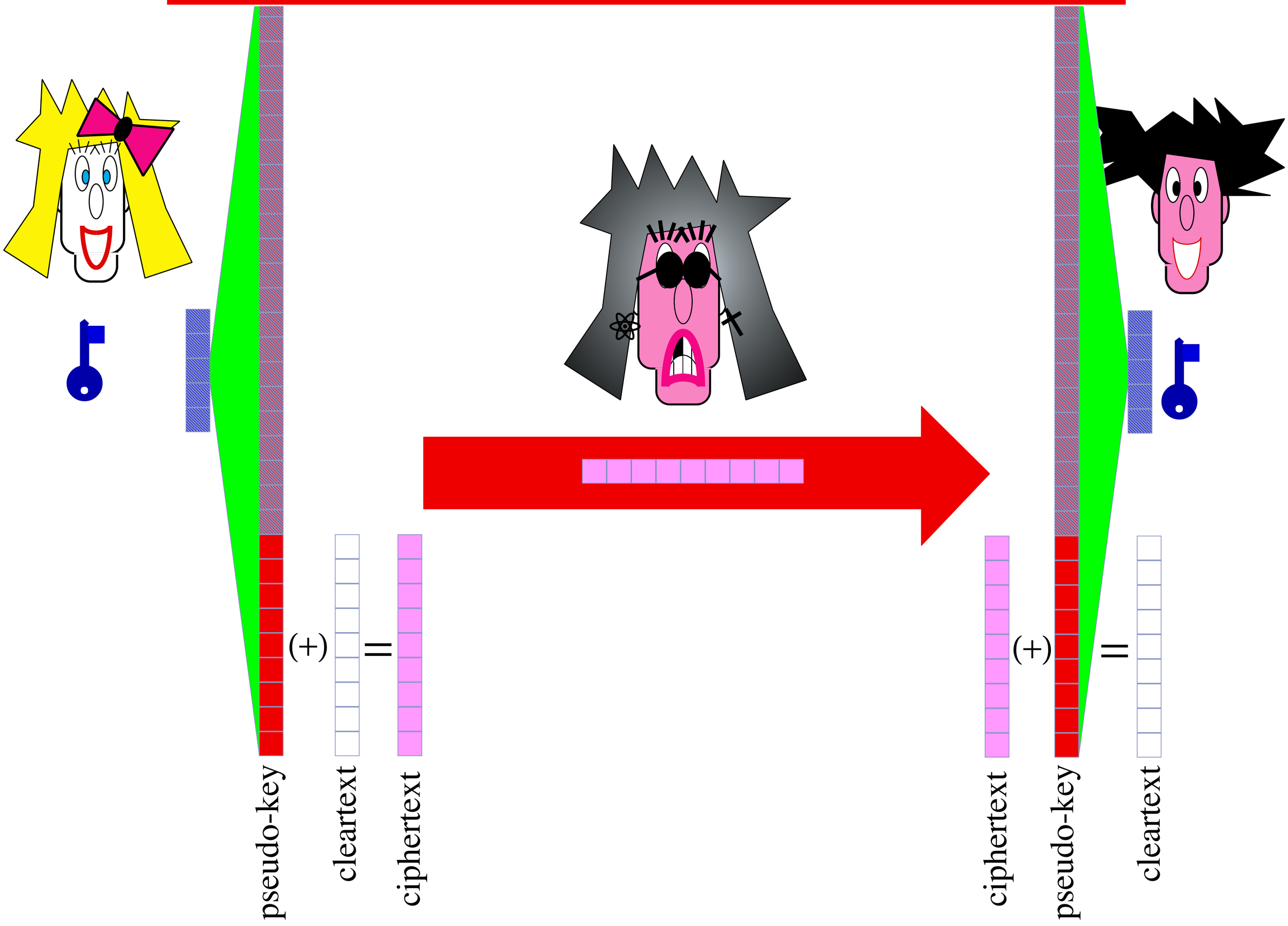


Pseudo-random bit generator

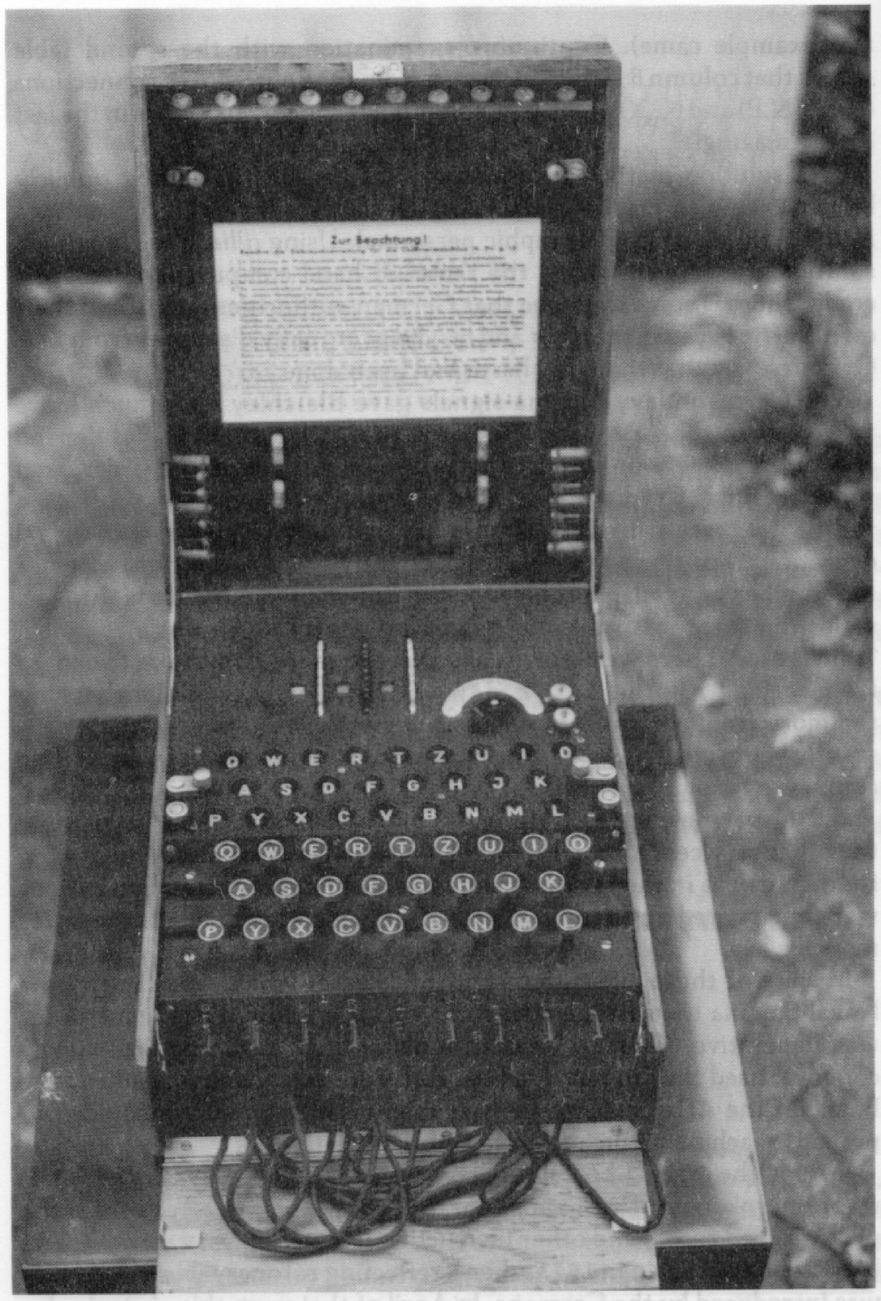


encryption

Stream-cipher from PRBG

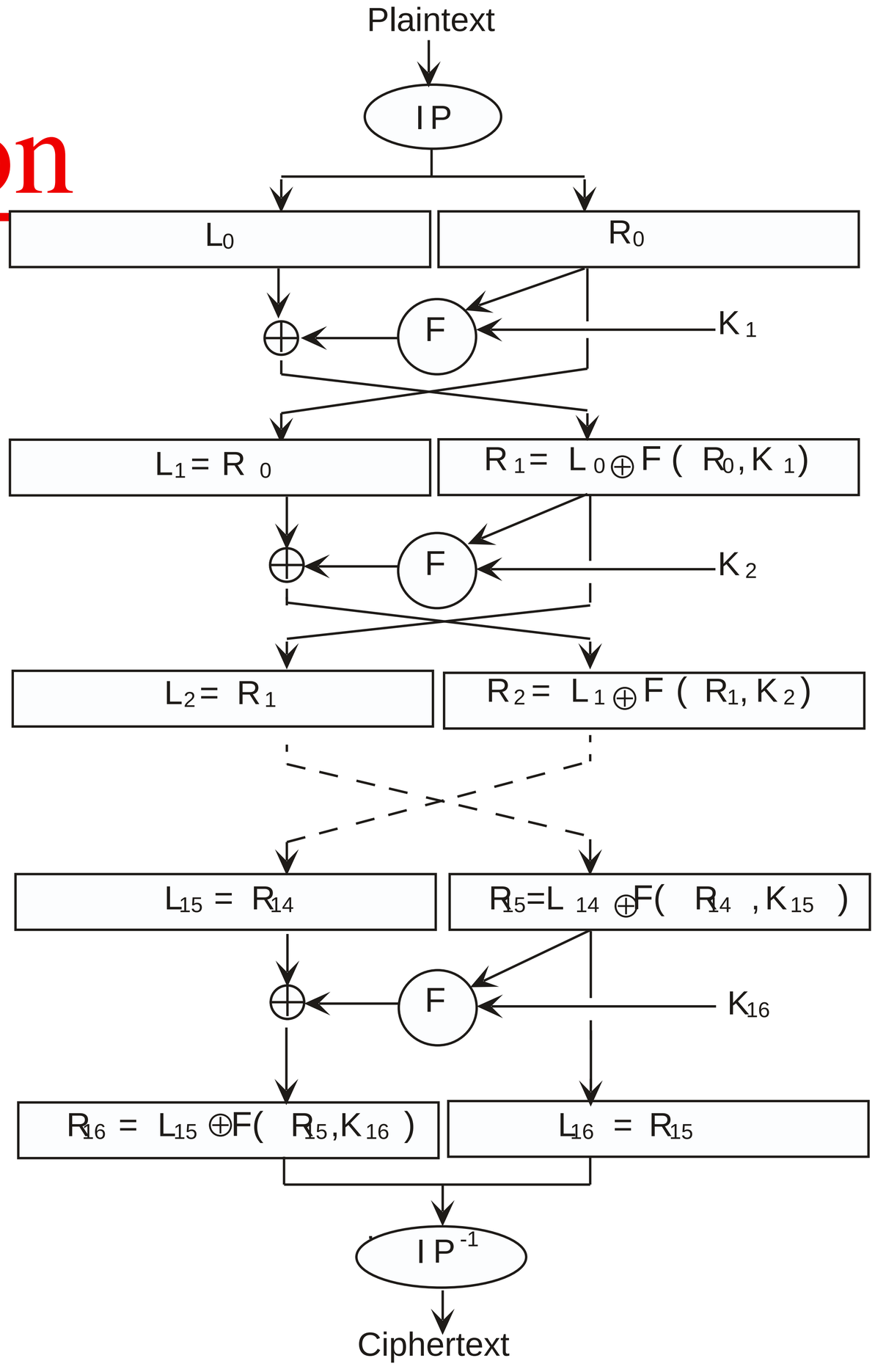


ENIGMA



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

Data Encryption Standard



Advanced Encryption Standard

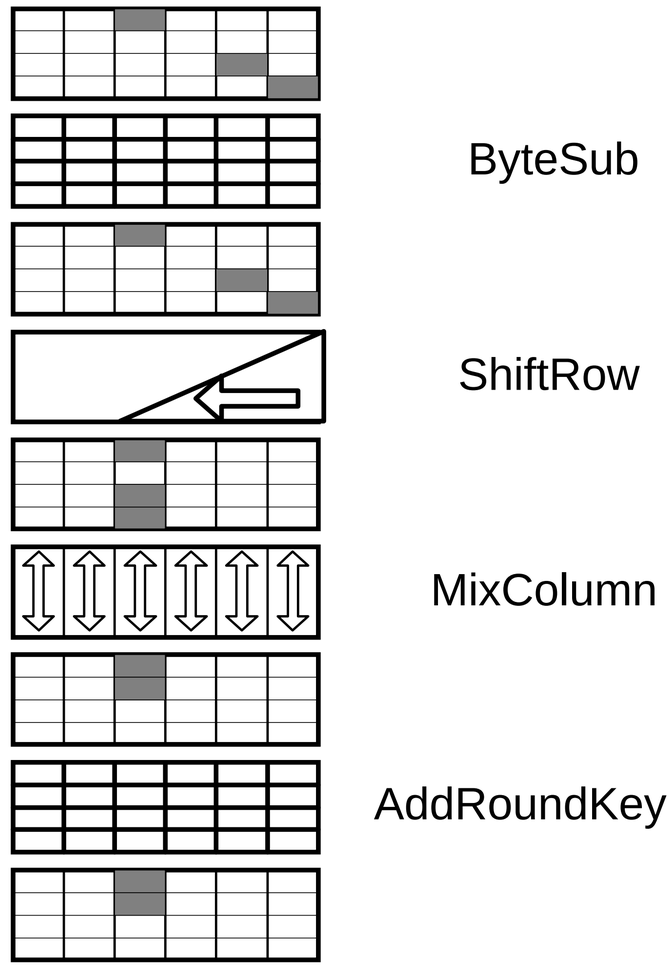
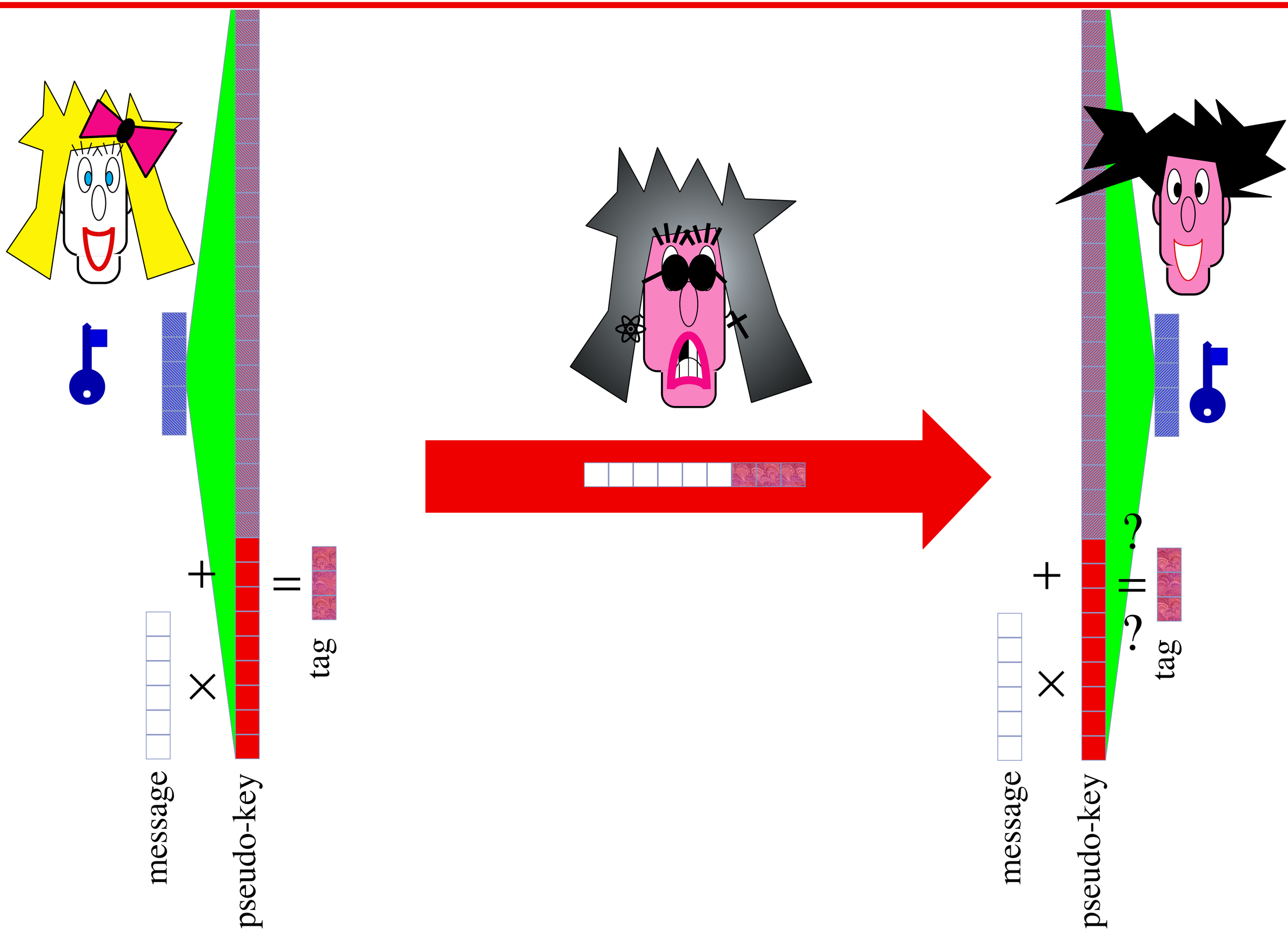


Figure 7: Propagation of activity pattern (in grey) through a single round

authentication

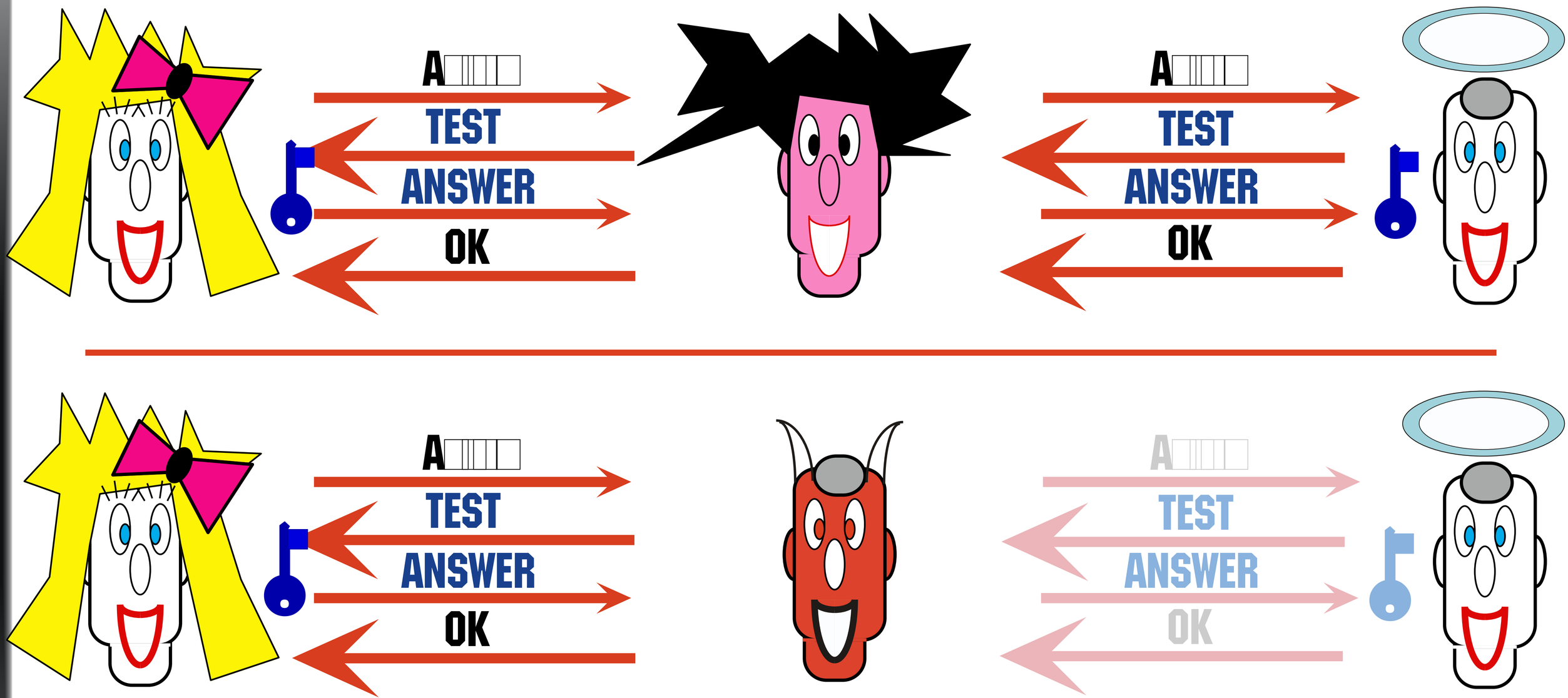
One-Time-Authentication from PRBG



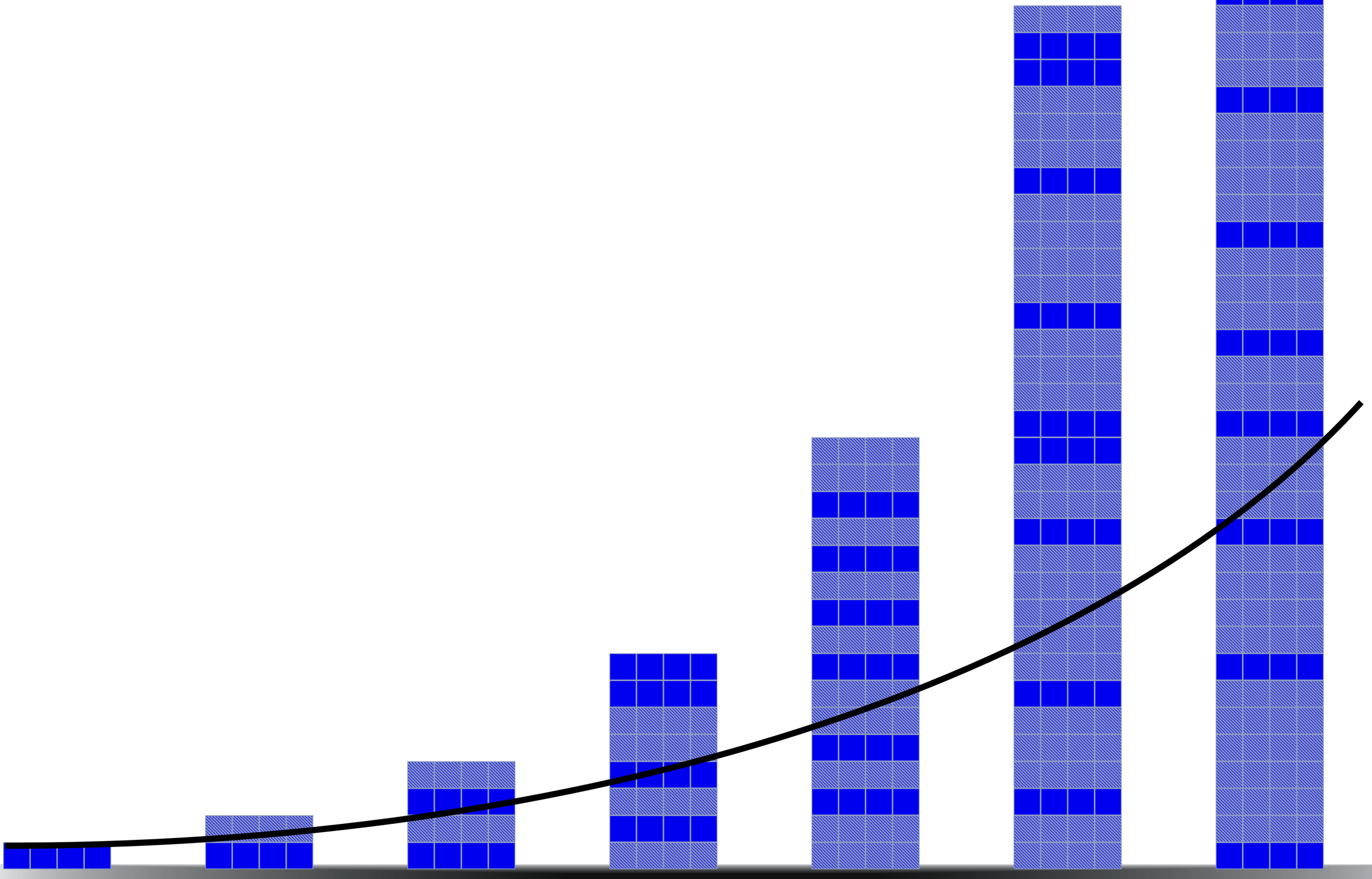
Message Authentication Codes (MACs)

identification

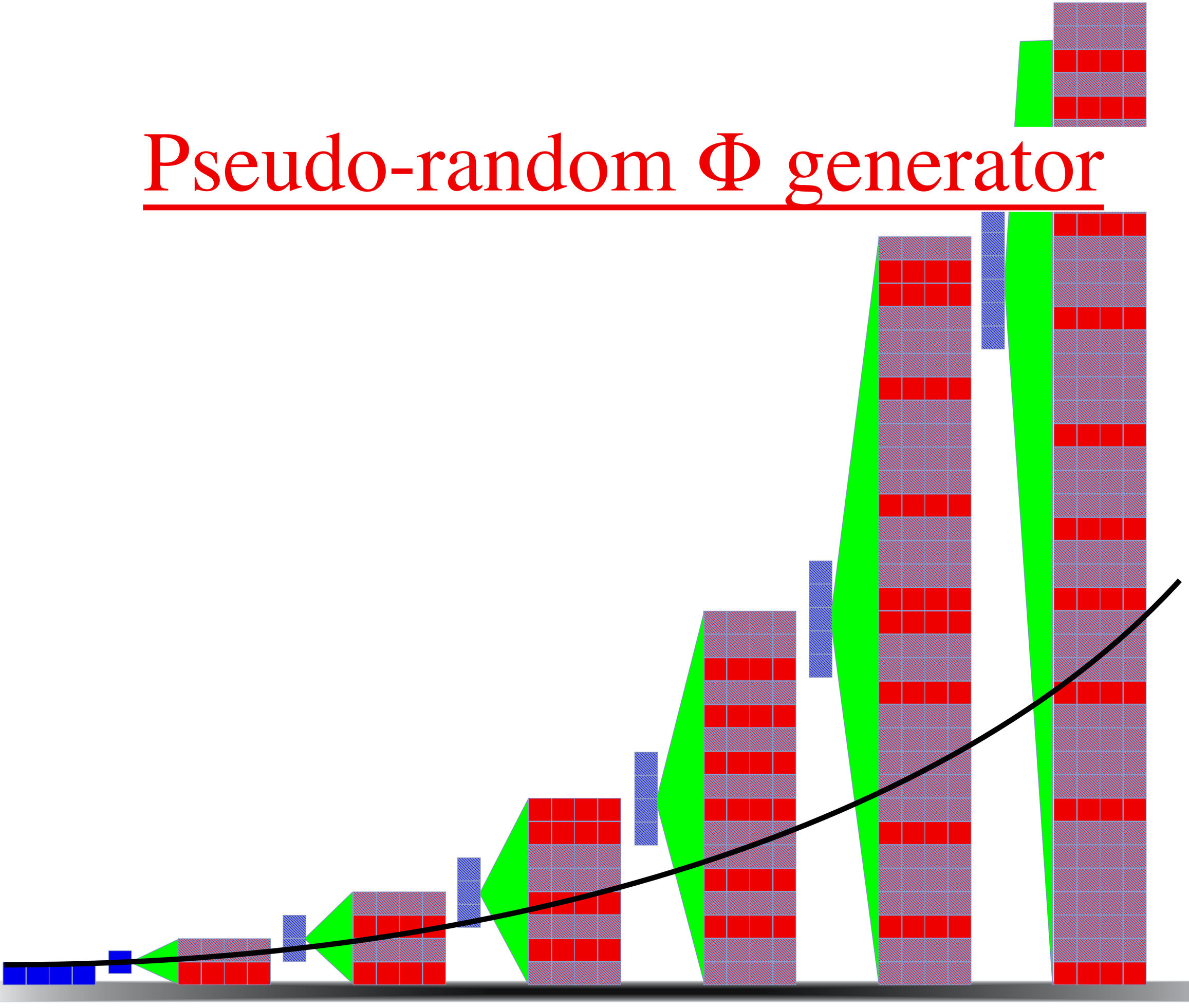
on-line identification



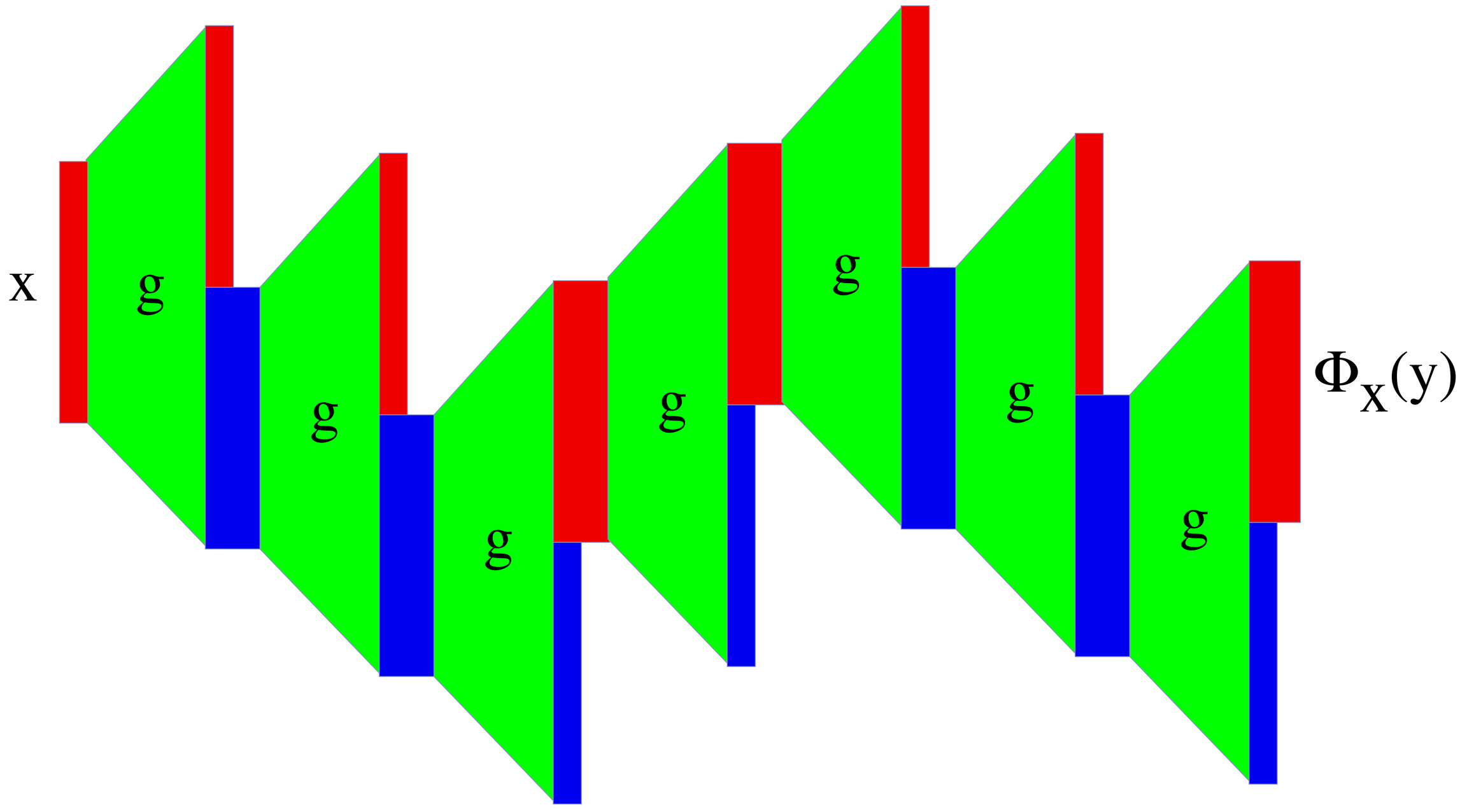
Truely random func



Pseudo-random Φ generator



Pseudo-random Φ generator



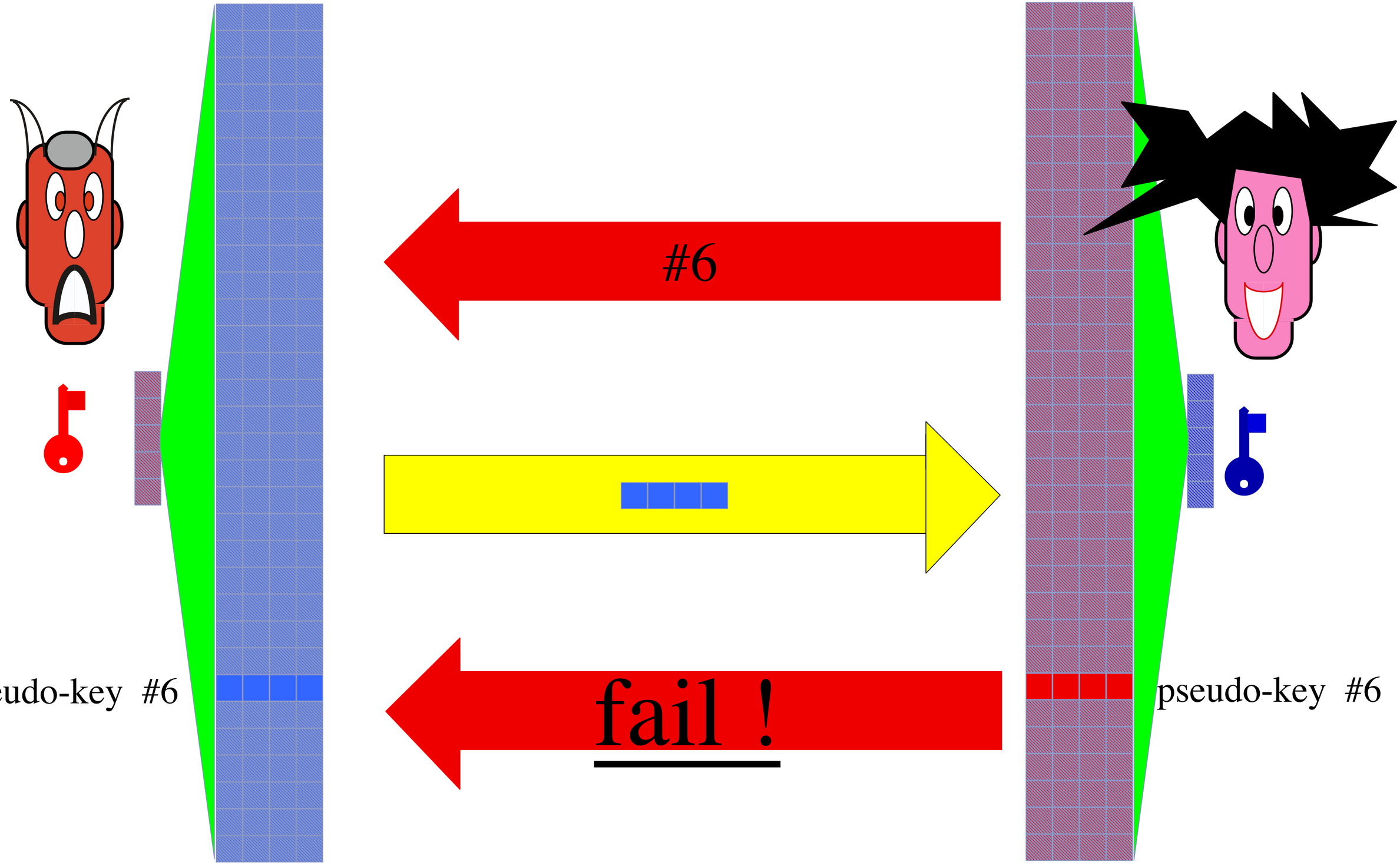
#6

pseudo-key #6

OK !

pseudo-key #6

Identification from PRΦG



Identification from PRΦG

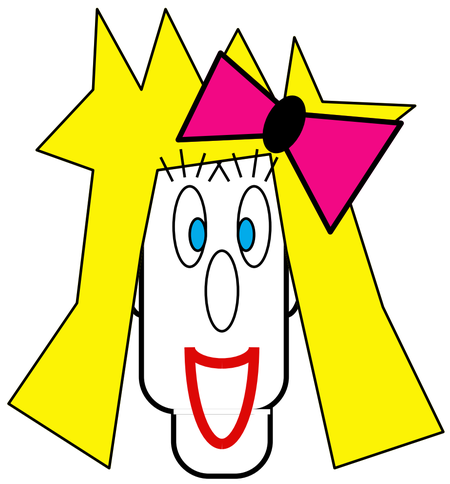
COMP-199

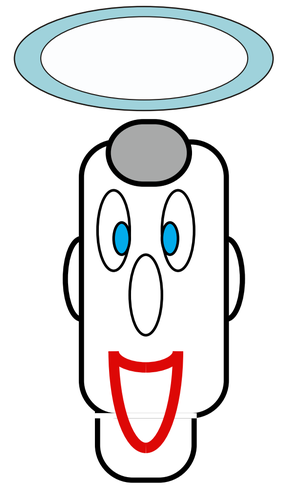
Introduction to Cryptography

Lecture 02

Claude Crépeau

School of Computer Science
McGill University





CIAO !