# COMP-199

## Introduction to Cryptography

## Lecture 03

**Claude Crépeau**

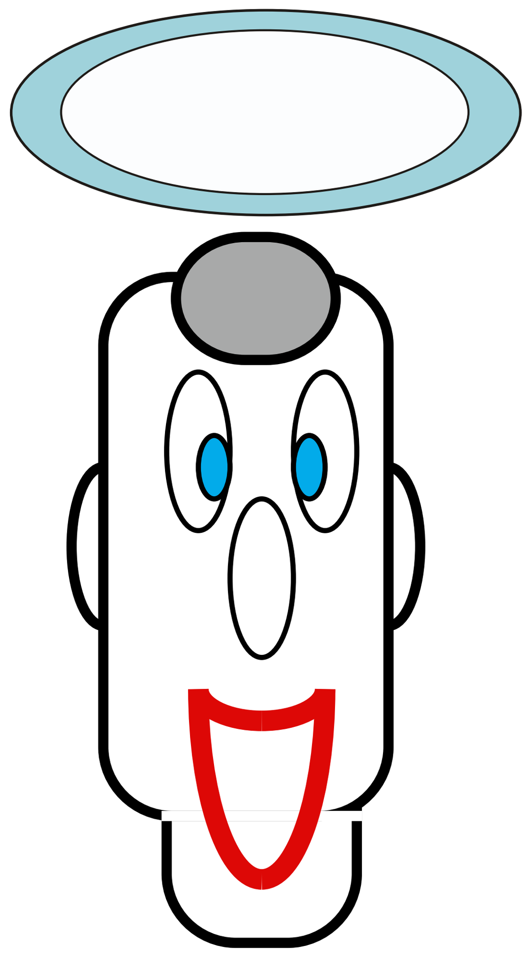
School of Computer Science
McGill University

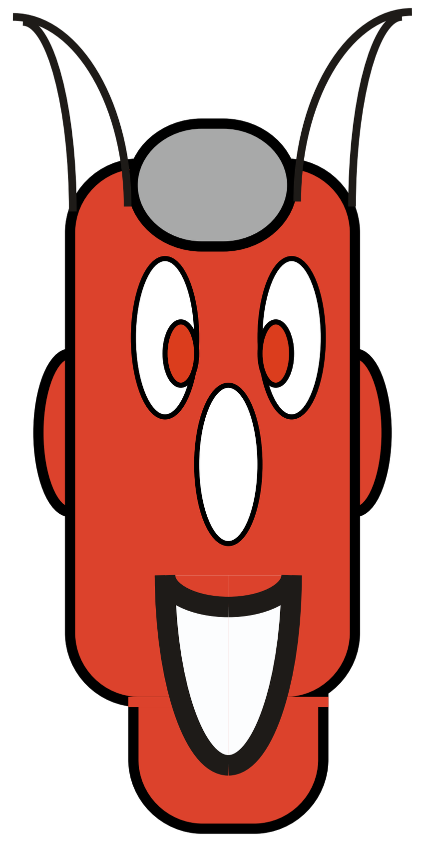
# Complexity

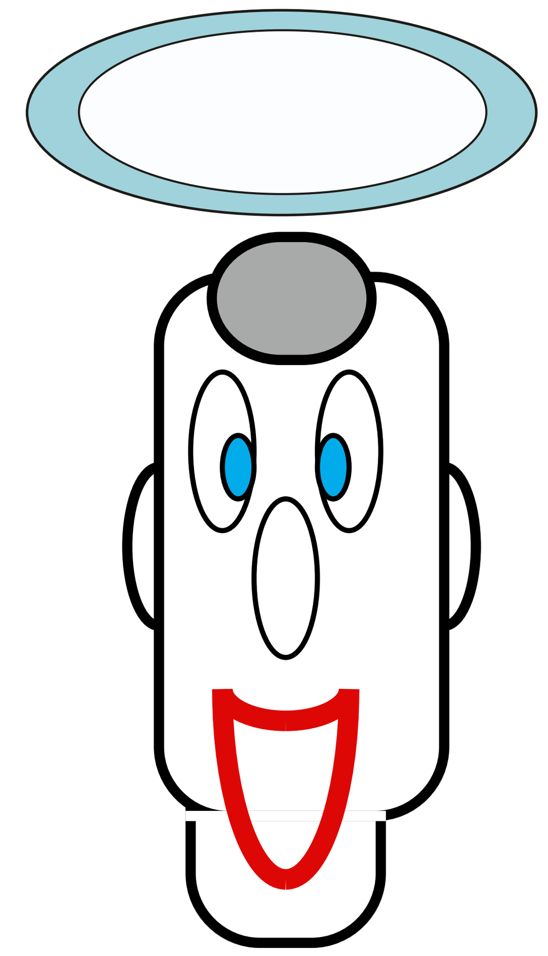
# Theoretical

# Cryptography

# Complexity Theoretical Asymmetric Cryptography







.....

public key distribution

asymmetric encryption

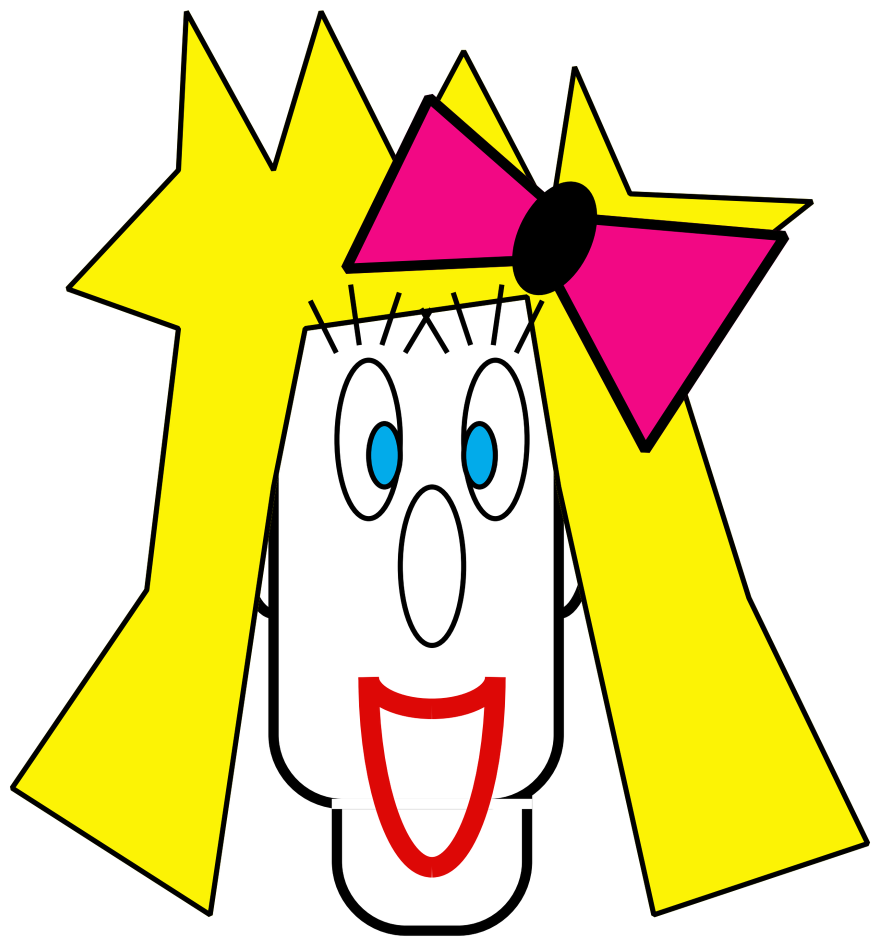
asymmetric authentication

zero-knowledge identification

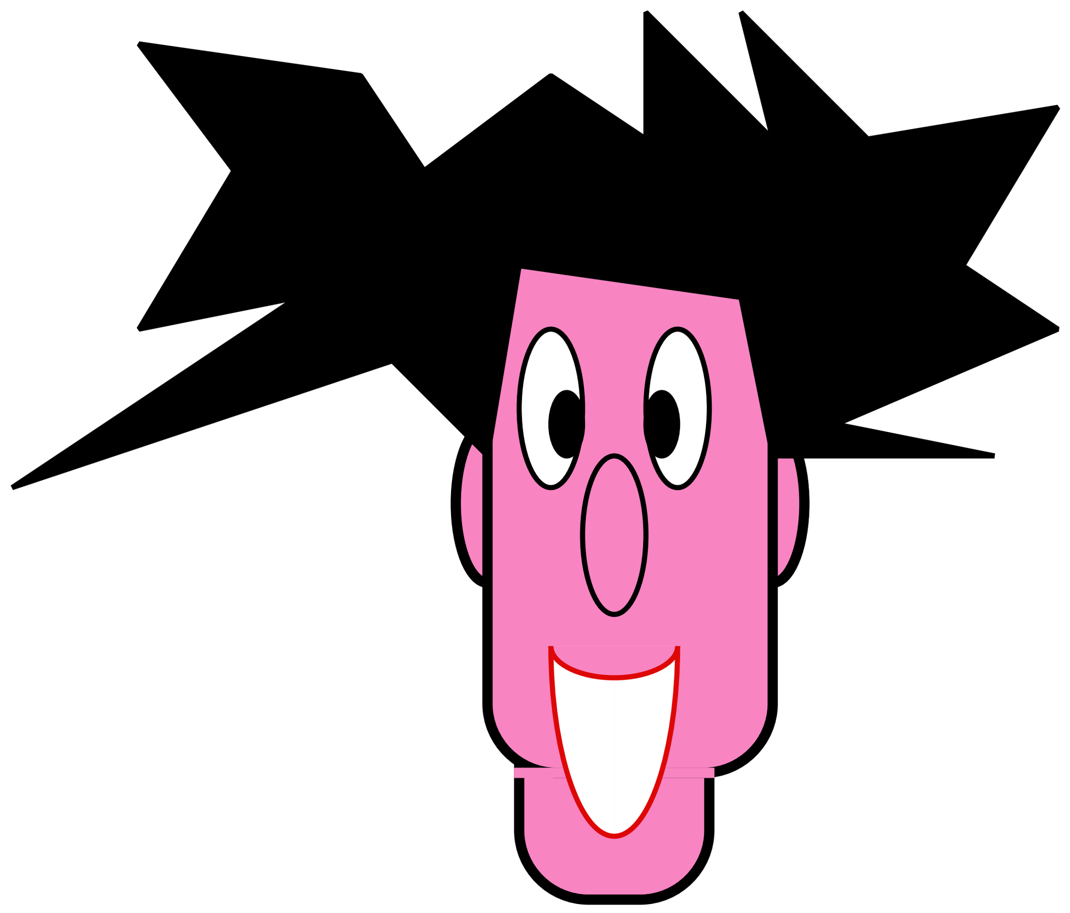
.....

# public key distribution

# PUBLIC-KEY DISTRIBUTION

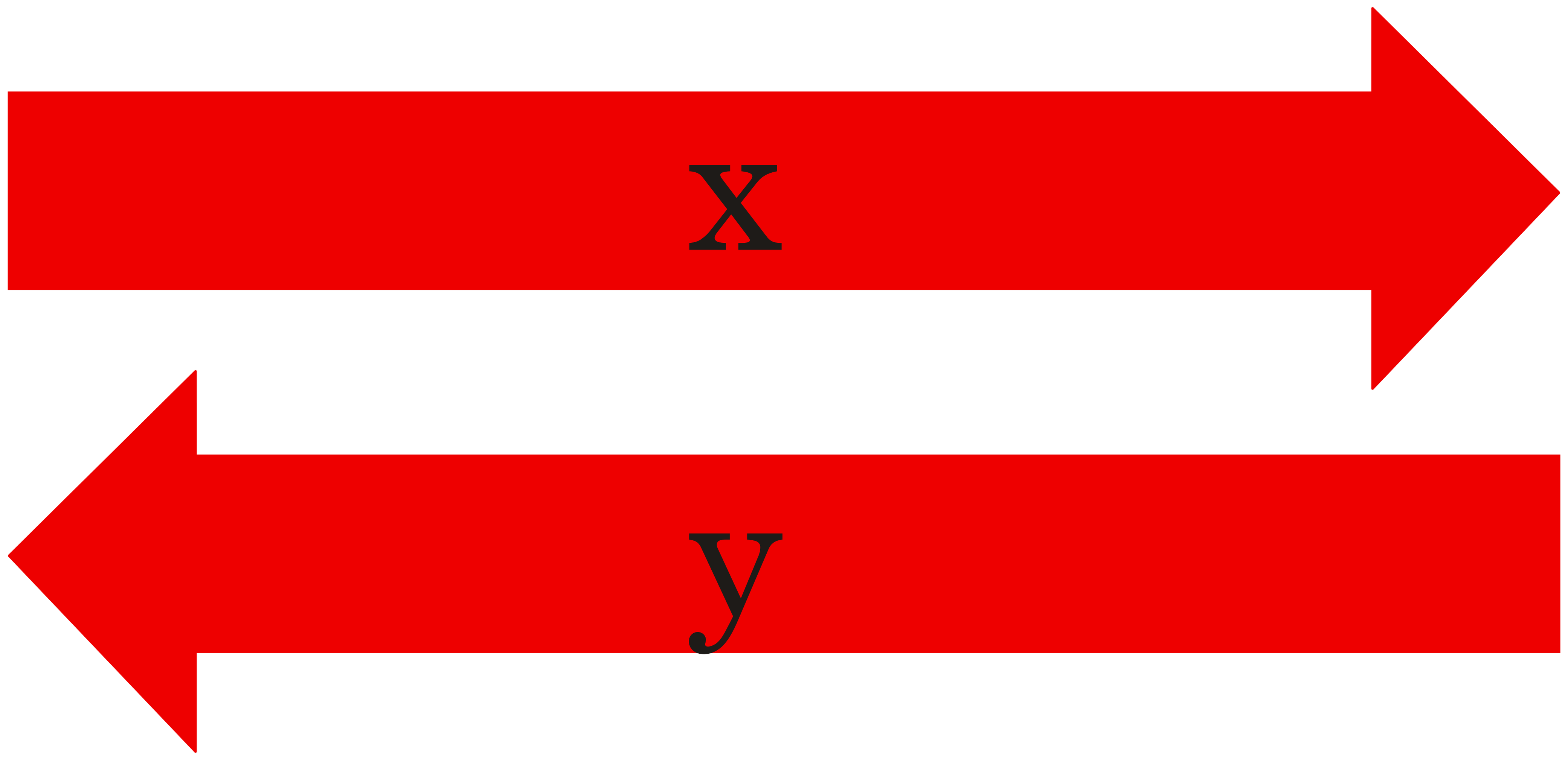


p



$x := f(p, a)$

$y := f(p, b)$




$k := f(y, a)$

$k := f(x, b)$

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

# modular arithmetic

- a+b **mod** n

running time: $O(|n|)$

- a*b **mod** n

running time: $O(|n|^2)$

- (+,*) field **mod** p

associative - commutative - distributive - inverses

- generators **mod** p

$\{g^1 \textbf{mod } p, g^2 \textbf{mod } p, \ldots, g^{p-1} \textbf{mod } p\} = \{1,2,\ldots,p-1\}$

# computing $a^e$ **mod** n

expo(a,e,n: integer):integer

x := 1
**WHILE** e>0 **DO**
. . . **IF** e is odd **THEN** x := ax **mod** n
. . . a := $a^2$ **mod** n
. . . e := e **div** 2
**RETURN** x

running time: $O(|n|^2 \, |e|)$

# testing pseudo-primality

pseudo(a,n: integer):boolean

**IF** gcd(a,n)>1 **THEN RETURN** F
compute s,t such that $n-1 = t2^s$ (t odd)
$x := a^t$ **mod** n; y := 1
**WHILE** s>0 and x>1 **DO**
. . . y := x; $x := x^2$ **mod** n; s := s-1
**IF** x>1 or 1<y<n-1 **THEN RETURN** F
**ELSE RETURN** T

running time: $O(|n|^3)$

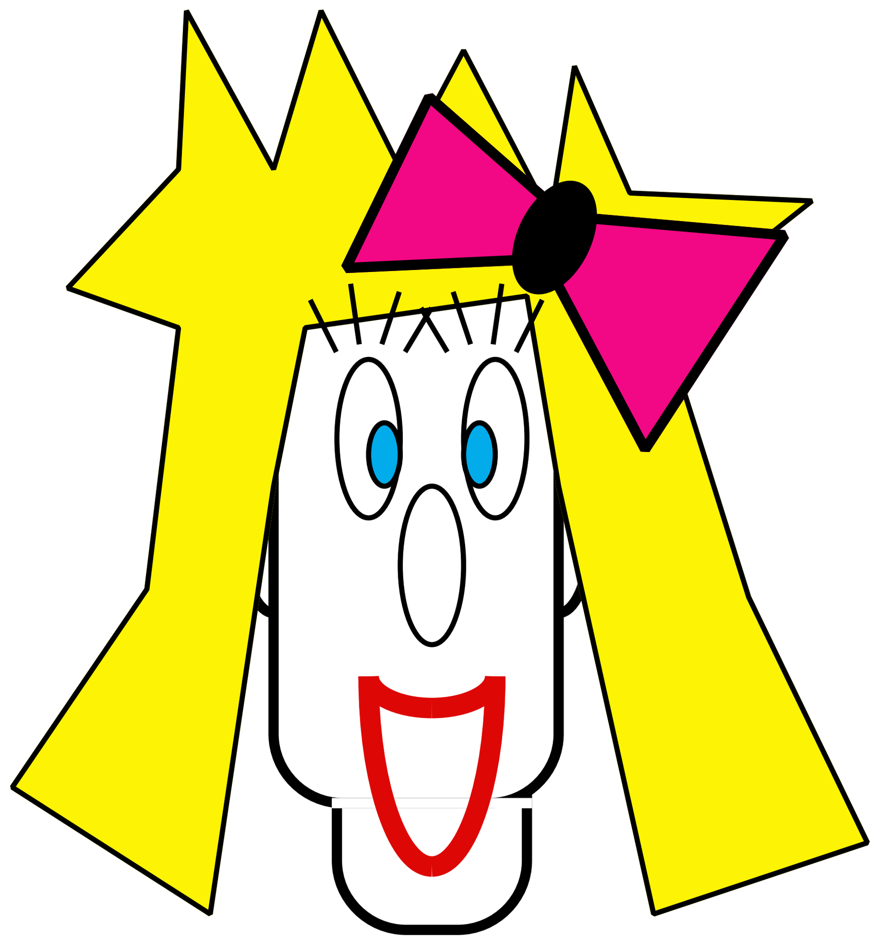
# testing a generator

gen(g,p: integer):boolean

**IF** $g^{p-1}$ **mod** p>1 **THEN RETURN** F
**FOREACH** q prime factor of p-1 **DO**
. . . **IF** $g^{p-1/q}$ **mod** p=1 **THEN RETURN** F
**ELSE RETURN** T

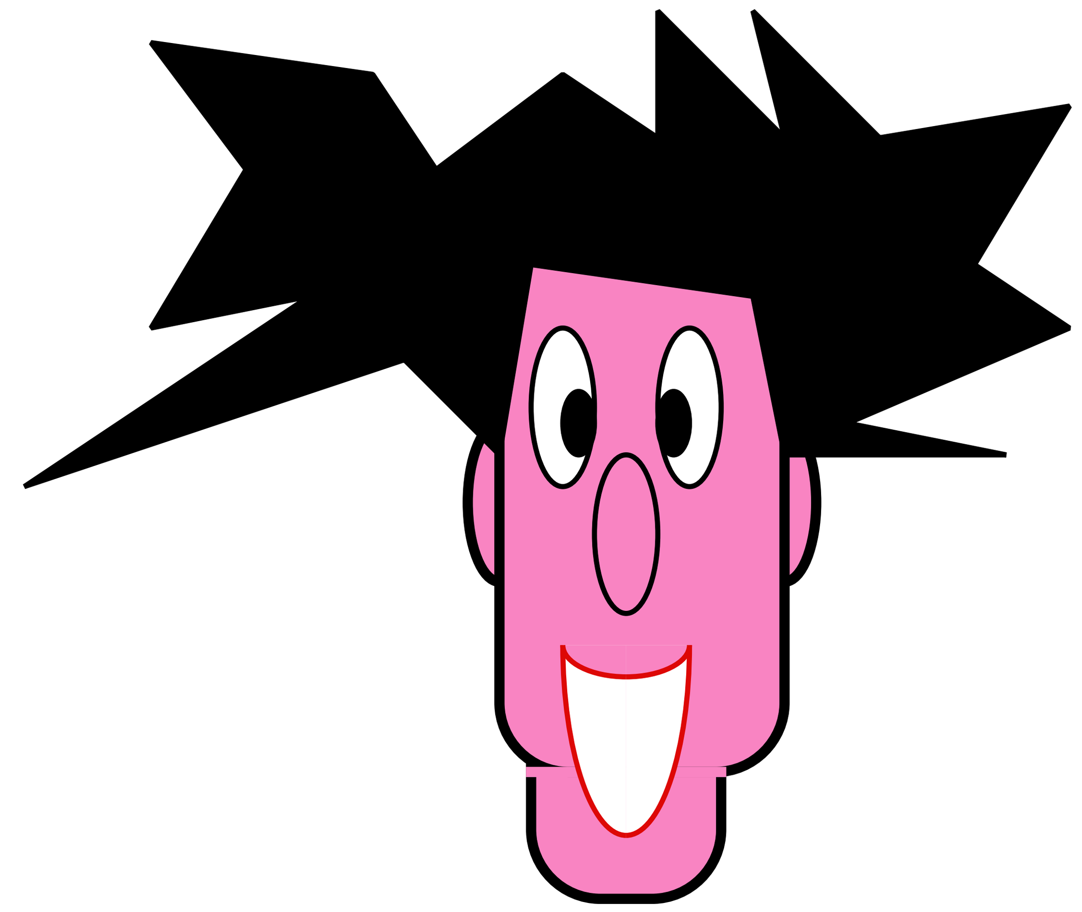
running time: $O(|n|^3 \log |n|)$ given the q's
density of generators $< p \approx p/\ln |p|$

# PUBLIC-KEY DISTRIBUTION



p: prime

g: generator



$x := g^a \bmod p$ $\qquad$ $y := g^b \bmod p$

x →

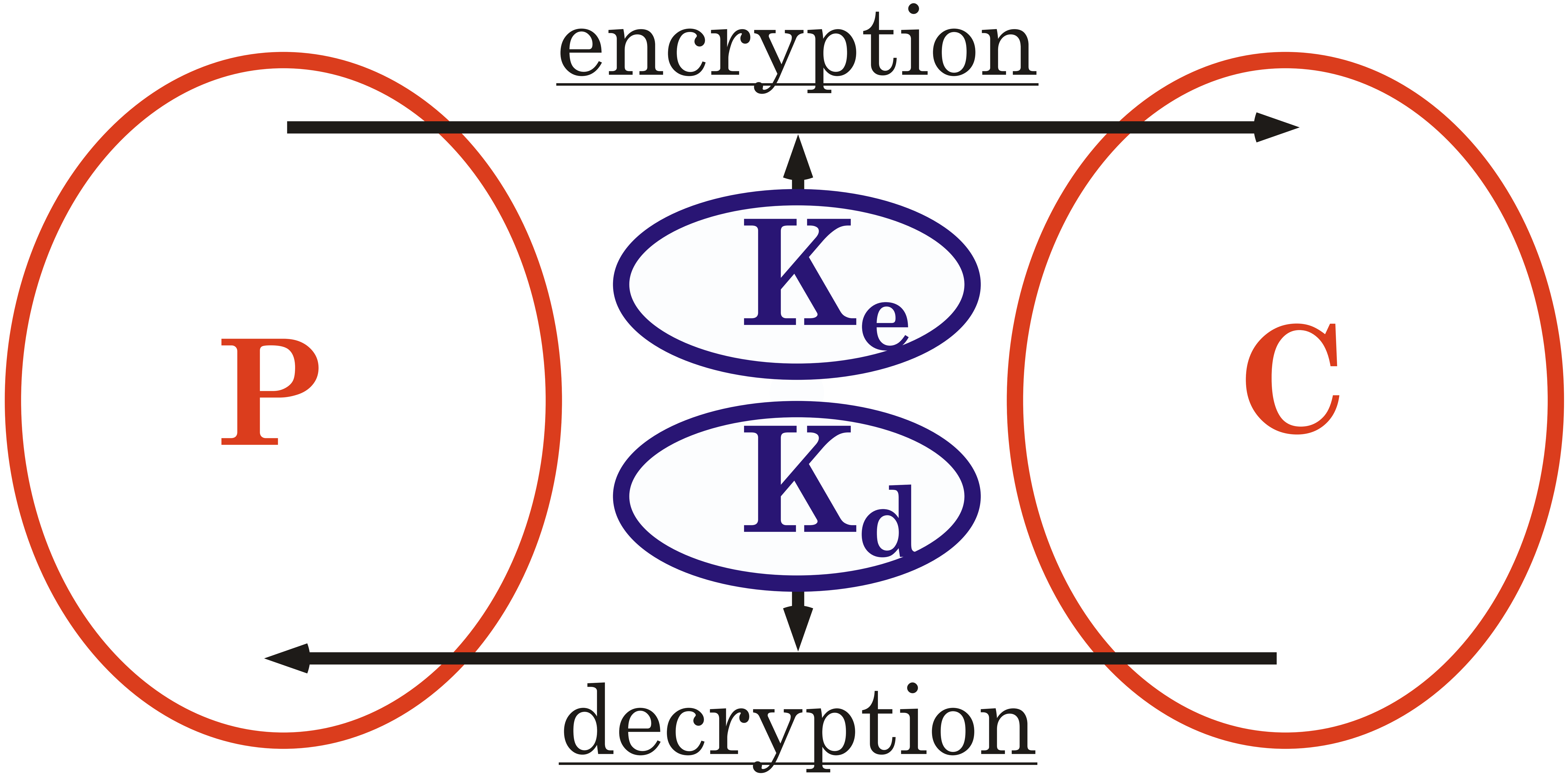
← y

$k := y^a \bmod p$ $\qquad$ $k := x^b \bmod p$

$$((g^a)^b) = k = ((g^b)^a)$$

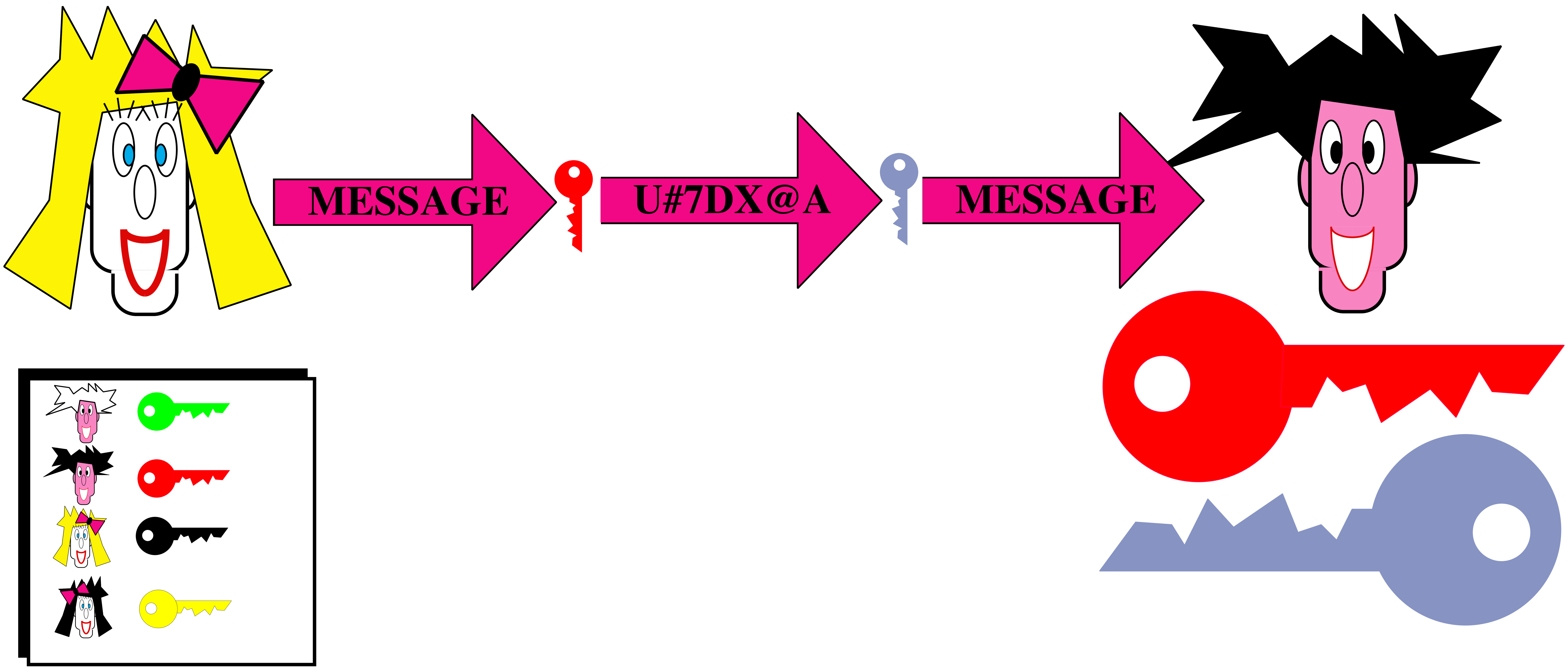
public key encryption

# asymmetric encryption
## (public-key cryptography)




**Complexity Theoretical Security**

# PUBLIC-KEY CRYPTOGRAPHY



# RSA public-key cryptosystem

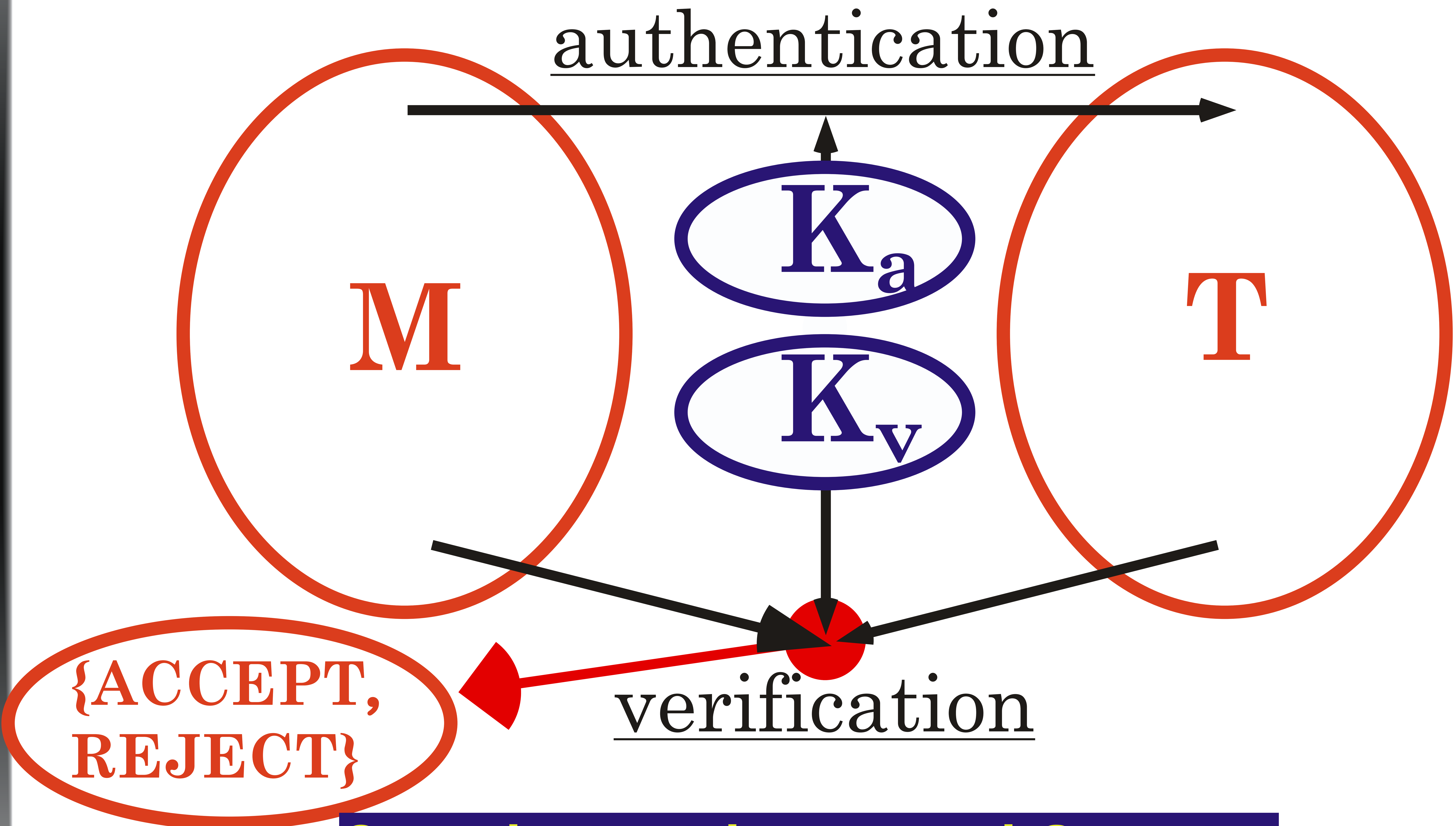
- $n = p*q$, two large primes
- e such that $gcd(e,(p-1)(q-1))=1$
- d such that $e*d = 1$ **mod** $(p-1)(q-1)$
- $K_e = (n,e)$, $K_d = (n,d)$
- **encryption** $E(m)$: $m^e$ **mod** n
- **decryption** $D(c)$ : $c^d$ **mod** n

# Various PKCS

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

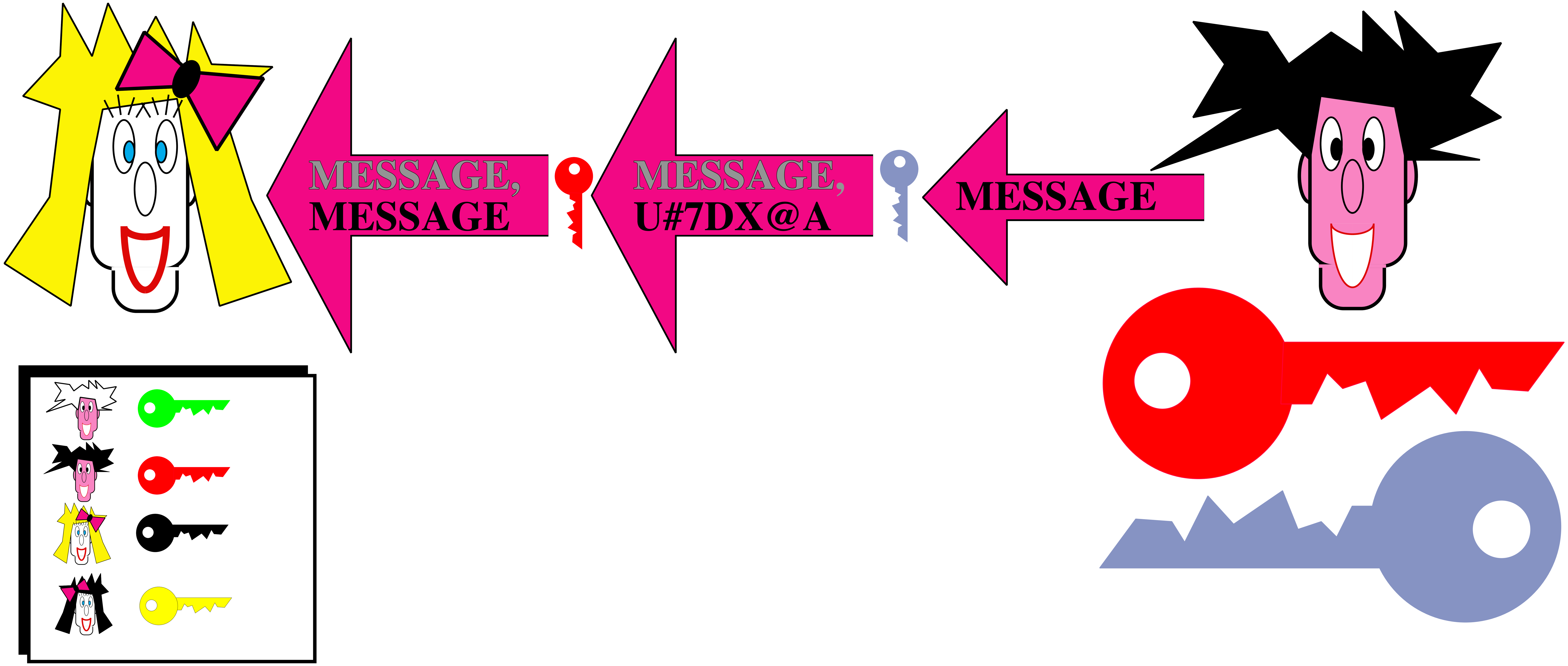
# digital signatures

# asymmetric authentication
## (digital signature schemes)




**Complexity Theoretical Security**

# Digital Signature



# RSA digital signature scheme

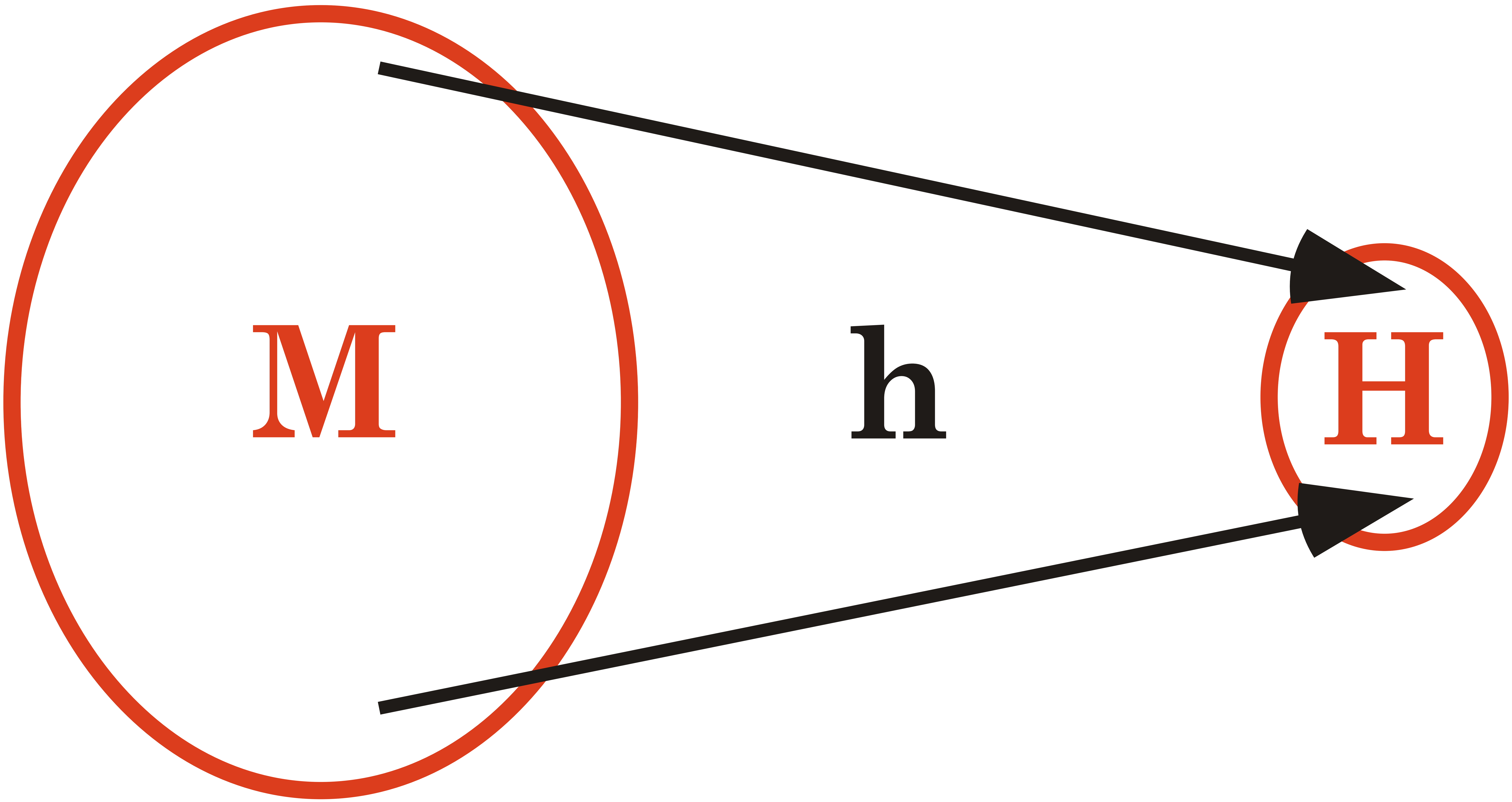
- n = p*q,   two large primes
- v such that gcd(v,(p-1)(q-1))=1
- a such that v*a = 1 **mod** (p-1)(q-1)
- $K_a = (n,a)$, $K_v = (n,v)$
- **Authentication** A(m): $m^a$ **mod** n
- **Verification**   V(m,t): $m=t^v$ **mod** n

# Various Digital Signatures

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

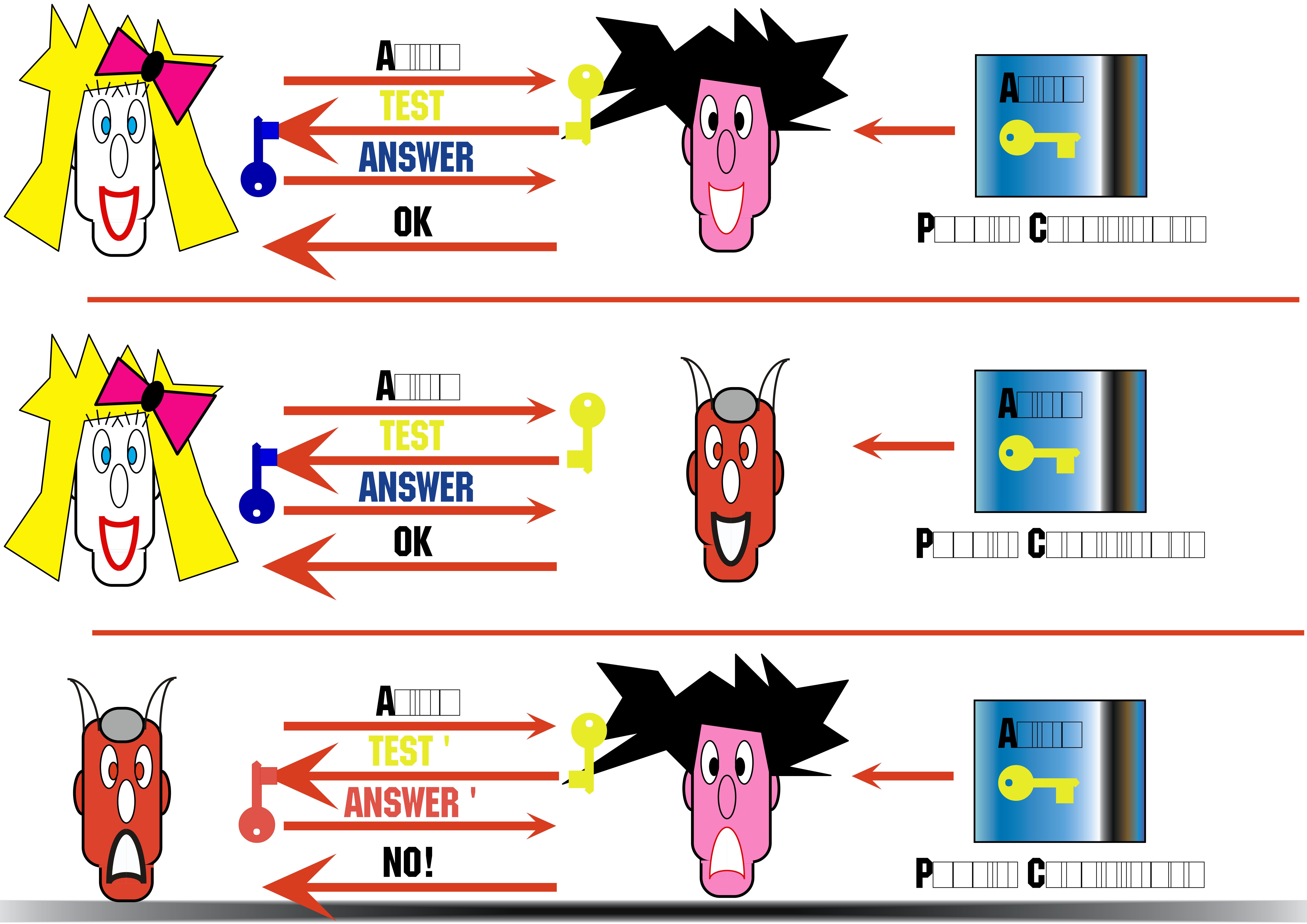
# Message Digest

## (cryptographic hashing)



# zero-knowledge identification

# off-line solution



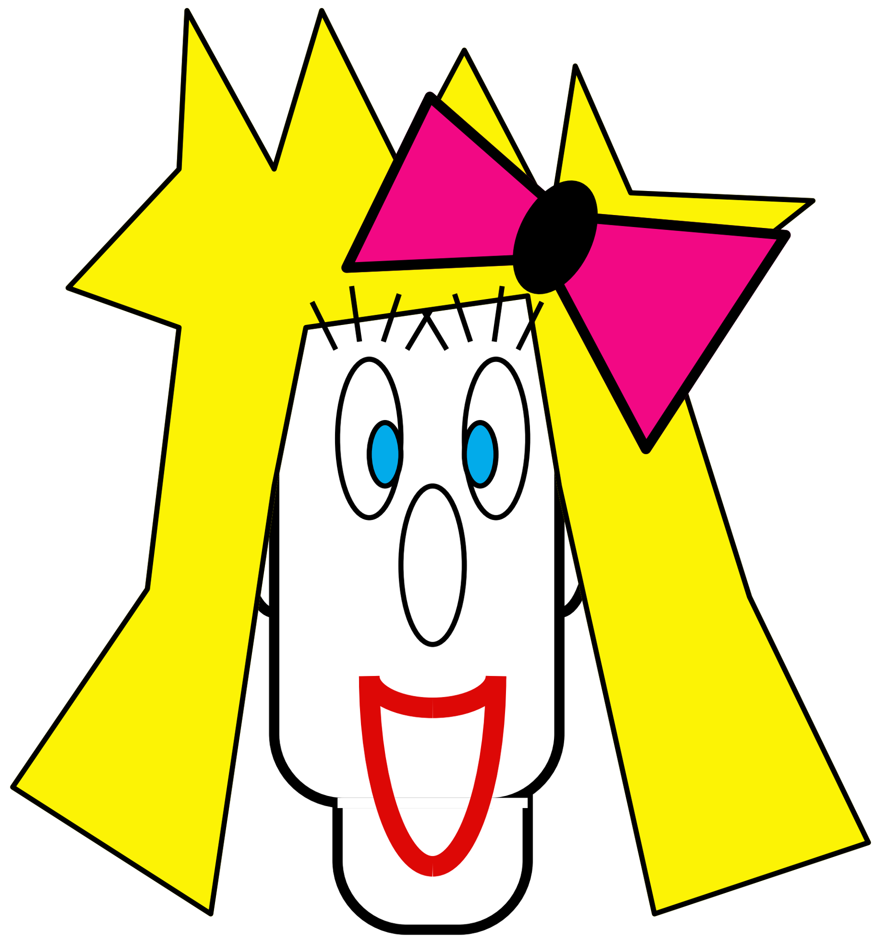
# COMP-199

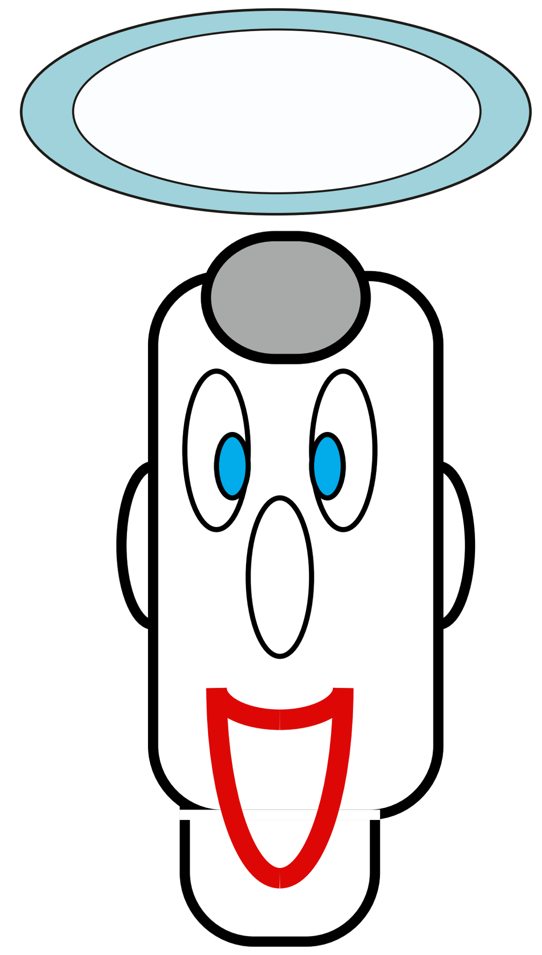
## Introduction to Cryptography

## Lecture 03

**Claude Crépeau**

School of Computer Science
McGill University





# CIAO !