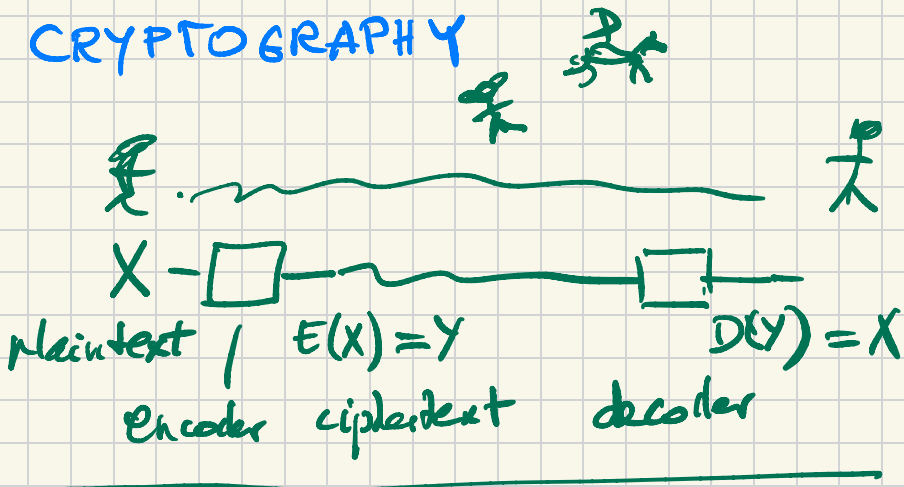
CRYPTOGRAPHY



1978 "PUBLIC KEY"

knowing E has full info about D

```
for all X
    compute E(X)
    if E(X)=Y
    return X
```

} exponential time

E, D efficiently computable
$ED = I_X$ $DE = I_Y$
given E. for almost all Y D(Y) is hard to compute

1978 RONALD RIVEST. ADI SHAMIR. LEONARD ADLEMAN

RSA

based on assumed hardness of factoring integers

p, q n-digit primes

given pq compute $\{p, q\}$

$\exp(O(\sqrt{n}))$

recommended movies

SNEAKERS

2001 SPACE ODYSSEY ↩

better than movie:

read novel by

ARTHUR C. CLARKE

FERMAT'S LITTLE THM

$$(\forall a \not\equiv 0 \bmod p)\left(a^{p-1} \equiv 1 \bmod p\right)$$

$p \nmid a$

p does not divide a

COR $M := (p-1)(q-1)$

$$(\forall a)_{\forall k}\left(a^{kM+1} \equiv a \bmod pq\right)$$

EX. $22^{70} \equiv 1 \bmod 71$

$p \neq q$ primes find e, f

$N := pq$

PUBLISH N, e

keep f private

discard p, q

$ef \equiv 1 \bmod M$

$E(X) = (X^e \bmod N)$

$D(y) = (y^f \bmod N)$

$\therefore X^{ef} \equiv X \bmod N$

$y^{ef} \equiv y$

Modular exponentiation

INPUT a, b, m

OUTPUT $(a^b \bmod m)$

$A := 1$

for $i = 1$ to b

$A := (aA \bmod m)$

return A

multiplications : b n-digit

$b \approx 2^n$

$a^{135} = a^{128} \cdot a^4 \cdot a^2 \cdot a^1$ $\quad 135 = 128 + 4 + 2 + 1$

$128 = 2^7$ $\quad a, a^2, a^4, \ldots, a^{128}$

7 multip.

Repeated squaring

INPUT: a, b, m pos. integers

X, A, B $\quad$ X: accumulator

Init: $X := 1,\ B = b,\ A = a$

while $B \geq 1$

if B odd **then** $B := B-1,\ X := (AX \bmod m)$

else $\quad B := B/2 \quad A := (A^2 \bmod m)$

return X

Ex. loop invariant

$$X A^B \equiv a^b \bmod m$$

$\therefore$ if $B = 0$ then $X = a^b$

Decision problem: binary OUTPUT Y/N T/F 1/0

FACT problem:

Input: a, b

Question: does a have a nontrivial divisor $\leq b$

how to reduce factoring to FACT

factor a

given black box for FACT

factor a

~~$\sqrt{a}$ has $\frac{1}{2}$ digit~~

Solution: binary search