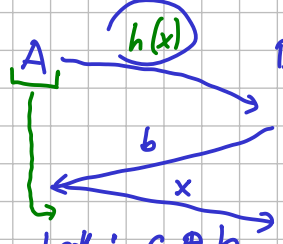
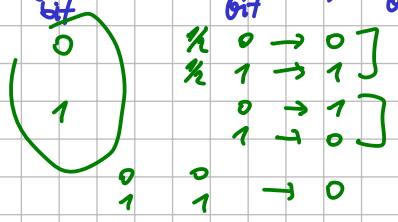
Tossing a coin over a phone call



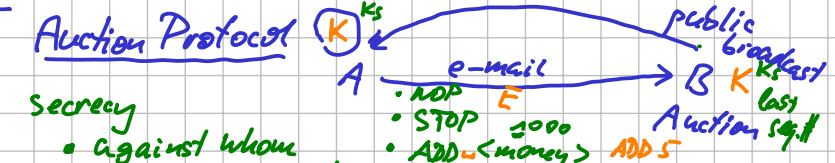
A: $x \in_R \{0,1\}^{128}$

bit commitment protocol

any fixed bit ⊕ random bit → random bit



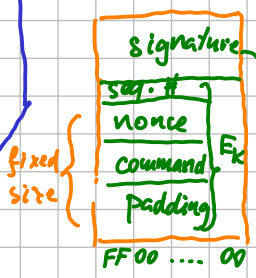
Auction Protocol



secrecy
- against whom
- for how long

symmetric cipher setup for a key

replay attack



Message Authentication Code (MAC)

h(Ks || encrypted part)

h(... ...) → key

Key Generation Function Derivation

session ID (nonce)

|| session ID

Kinds of attacks

- known ciphertext → recover plaintext
- known plaintext → recover key
- chosen plaintext
- distinguishing attack

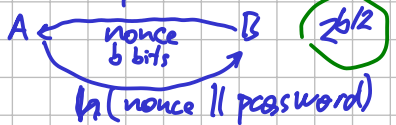
How to measure strength?

b: security level (bits)

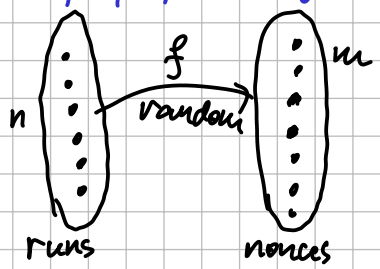
Attacker requires $\geq 2^b$ operations to break our protocol.

Birthday Attacks

Challenge-response auth scheme



23 people, 366 days → $Pr[\text{2 share a birthday}] \geq 1/2$



$$Pr_f[f \text{ injective}] = \frac{\#\text{inj. fcts}}{\#\text{all fcts}} = \frac{m \cdot (m-1)(m-2)\cdots(m-n+1)}{m^n} = \frac{m}{m} \cdot \frac{m-1}{m} \cdot \frac{m-2}{m} \cdots \frac{m-n+1}{m}$$

m^n

$$(1) \quad \left(1-\frac{1}{m}\right) \quad \left(1-\frac{2}{m}\right) \cdots$$

$1-x \approx e^{-x}$

$$\approx 1 \cdot e^{-\frac{1}{m}} \cdot e^{-\frac{2}{m}} \cdots e^{-\frac{n-1}{m}}$$

$$= e^{-\frac{1}{m} - \frac{2}{m} - \cdots - \frac{n-1}{m}}$$

$$= e^{-\frac{1+2+\cdots+n-1}{m}} \qquad 1+2+\cdots+n-1 = \frac{n(n-1)}{2}$$

$$= e^{-\frac{n(n-1)}{2m}} \approx e^{-\frac{n^2}{2m}}$$

$= \frac{1}{2}$

$$e^{-\frac{n^2}{2m}} = \frac{1}{2}$$

$$-\frac{n^2}{2m} = \ln\frac{1}{2}$$

$$\frac{n^2}{m} = -2 \cdot \ln\frac{1}{2} \doteq 1.38$$

$$n^2 \sim m$$

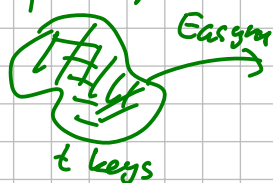
A → B: randomK

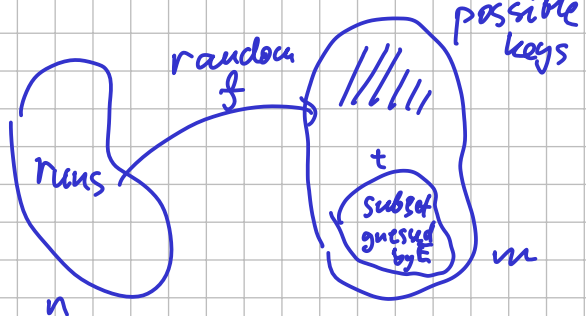
A → B: $E_{asym}(K, K^B_{pub})$

E: K_{guess}

$E_{asym}(K_{guess}, K^B_{pub}) \doteq$

precompute a table





$Pr_f[f \text{ avoids subset}] = \left(1-\frac{t}{m}\right)^n \approx e^{-\frac{tn}{m}}$

const. $\frac{1}{2}$

$tn \sim m$

e.g. $t := \sqrt{m}$, $n := \sqrt{m}$

sec. level $\leq \frac{\#\text{key bits}}{2}$

One-time Pad (Vernam's Cipher)

message: $x \in \{0,1\}^n$

key: $K \in_R \{0,1\}^n$ ↑ uniformly at random

ciphertext: $y = x \oplus K$

$[y_i = x_i \oplus k_i$ sequence of independent uniform random bit

decrypt: $y \oplus K = (x \oplus k) \oplus k =$

$= x \oplus (k \oplus k) = x$

Informational-theoretic security (perfect security)

1. One-time Pad
2. Secret sharing

n crazy generals

t threshold

if t generals meet → recover

< t → no inform. on S

↓

Symmetric ciphers