Complexity and Cryptography

A **Public-Key System** with key-pair $(\underline{e},\underline{d})$ consists of two functions $E=E(\underline{e},\underline{x})$ and $D=D(\underline{d},\underline{y})$ such that $D(\underline{d},E(e,\underline{x}))=\underline{x}$ holds for all $\underline{x}$.

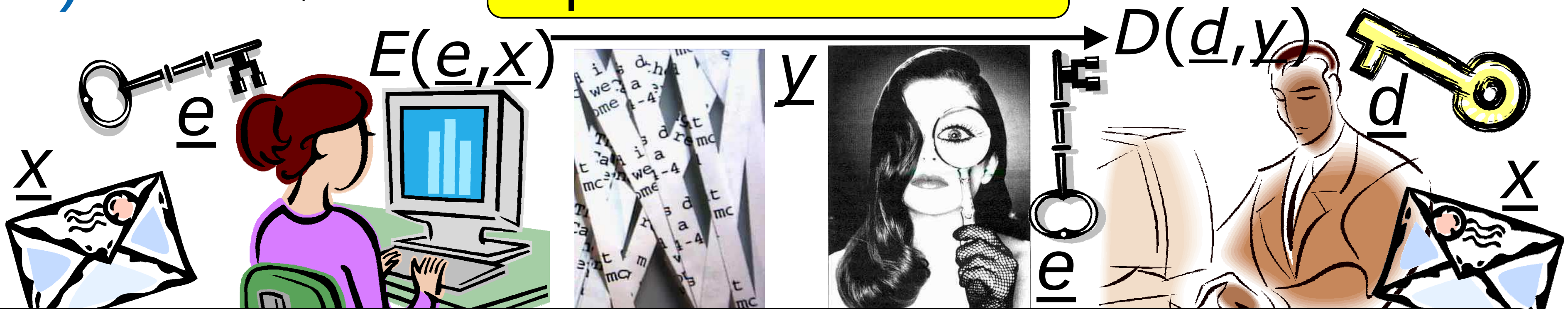
RSA

Call $f:\Sigma^*\to\Sigma^*$ a **one-way function** if

i) injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ for some k

ii) computable in polynomial time (i.e. $f\in\mathcal{FP}$)

iii) but $f^{-1}\notin\mathcal{FP}$ **impossible if $\mathcal{P}=\mathcal{NP}$!** $\Rightarrow f^{-1}\in\mathcal{FNP}$



encrypt with public key $\underline{e}$, decrypt with private key $\underline{d}$.

One-Way Functions and $\mathcal{UP}$

Definition: Call a NTM unambiguous if, for any input $\underline{x}$, it has at most one accepting computation.

$\mathcal{P} \subseteq \mathcal{UP} \subseteq \mathcal{NP}$

$\mathcal{UP}$ = {languages accepted by unambiguous polytime NTMs}

Theorem: $\mathcal{P} \neq \mathcal{UP}$ iff one-way functions exist.

Proof: a) For one-way f define $L := \{ (\underline{x},\underline{y}) \mid \exists \underline{z} \leq \underline{x}: f(\underline{z})=\underline{y} \}$

Then $L \in \mathcal{UP}$. And $\underline{y} \to f^{-1}(\underline{y})$ can be evaluated using binary search with polynomially many queries for L: $L \notin \mathcal{P}$

b) Let $L \in \mathcal{UP} \setminus \mathcal{P}$ be decided by unambiguous NTM U.

For $\underline{x}$ an accepting computation of U on $\underline{y}$, let $f(\underline{x}) := 1\underline{y}$.

For other arguments let $f(\underline{x}) := 0\underline{x}$.

This is one-way!

Call $f: \Sigma^* \to \Sigma^*$ a one-way function if injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ and $f \in \mathcal{FP}$ ($\Rightarrow f^{-1} \in \mathcal{FNP}$) but $f^{-1} \notin \mathcal{FP}$

Issues with Cryptographic Complexity

Definition: Call a NTM unambiguous if, for any input $\underline{x}$, it has at most one accepting computation. $\mathcal{P} \subseteq \mathcal{UP} \subseteq \mathcal{NP}$

$\mathcal{UP}$ = {languages accepted by unambiguous polytime NTMs}

Theorem: $\mathcal{P} \neq \mathcal{UP}$ iff one-way functions exist.

- It might be $\mathcal{P} = \mathcal{UP} \neq \mathcal{NP}$
- No complete problem known for $\mathcal{UP}$

Cannot eff. check whether given NTM is unambiguous

- *worst-case* complexity:

  f might be efficiently invertible on *many* practical inputs

- randomized algorithms are not deterministic yet practical

Call $f:\Sigma^*\to\Sigma^*$ a one-way function if injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ and $f \in \mathcal{FP}$ ($\Rightarrow f^{-1} \notin \mathcal{FNP}$) but $f^{-1} \notin \mathcal{FP}$

Simple Probabilistic Algorithm

Example: MaMu := $\{ (A,B,C)\in\mathbb{Z}_2^{3(m\times m)} : m\in\mathbb{N}, C=A\cdot B \}$

- deterministic algorithm: running time $O(m^3)=O(n^{1.5})$
- world record [Strassen],[Coppersmith&Winograd]: $O(m^{2.38})$
- randomized algorithm, running time $O(m^2)=O(n)$:
  - Guess $\underline{x}\in\mathbb{Z}_2^m$ identically independently at random
  - Calculate $\underline{y}:=B\cdot\underline{x}$, $\underline{z}:=A\cdot\underline{y}$, $\underline{w}:=C\cdot\underline{x}$.
  - If $\underline{w}=\underline{z}$, accept; otherwise reject.

Amplifiable to near certainty

Lemma: a) Every $(A,B,C)\in$ MaMu gets accepted.

b) A d-dimensional $\mathbb{Z}_2$-vector space has 2^d elements.

c) For $A,B,C\in\mathbb{Z}_2^{m\times m}$ with $C\neq A\cdot B$, dim kern$(C-A\cdot B)\leq m-1$

d) Each $(A,B,C)\notin$ MaMu is rejected with probability $\geq$½.

Randomized Algorithm for 3SAT

Uwe Schöning, Ulm

Sei $\underline{z}$ eine erfüllende Belegung von f

Mit Wahrscheinlichkeit $\binom{n}{\ell}\cdot 2^{-n}$ unterscheidet sich $\underline{y}$ von $\underline{z}$ an ℓ Stellen;

nach einem Durchlauf mit W'keit ⅓ nur noch an ℓ-1 Stellen, sonst an ℓ+1; erreiche $\underline{y}=\underline{z}$ mit Wahr'keit $\geq(⅓)^{\ell}$.

Wähle z.B. $\ell:=n/2$, $a:=40$, $b:=20\cdot 3^{n/2}$

besser $\ell:=n/4$, $b:=20\cdot 3^{\ell}$, $a:=20\cdot 2^{n}/\binom{n}{\ell}$.

Exponentialzeit algorithmen

Laufzeit $(1.33)^{n}\cdot \text{poly}(n)$

Gegeb. 3KNF Formel $f(x_1,\ldots,x_n)$

Wiederhole a-mal:

- rate Start-Belegung $\underline{y}\in\{0,1\}^{n}$
- Wiederhole $b\cdot n$-mal:
  - Falls $f(\underline{y})=1$, akzeptiere.
  - Sei C Klausel in f mit $C(\underline{y})=0$
  - Rate Literal x_k in C
  - und setze $y_k := 1-y_k$

Verwerfe.

$1/\binom{n}{cn} \approx c^{cn}\cdot(1-c)^{(1-c)n}$