Complexity and Cryptography

KAIST CS422 M. Ziegler

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

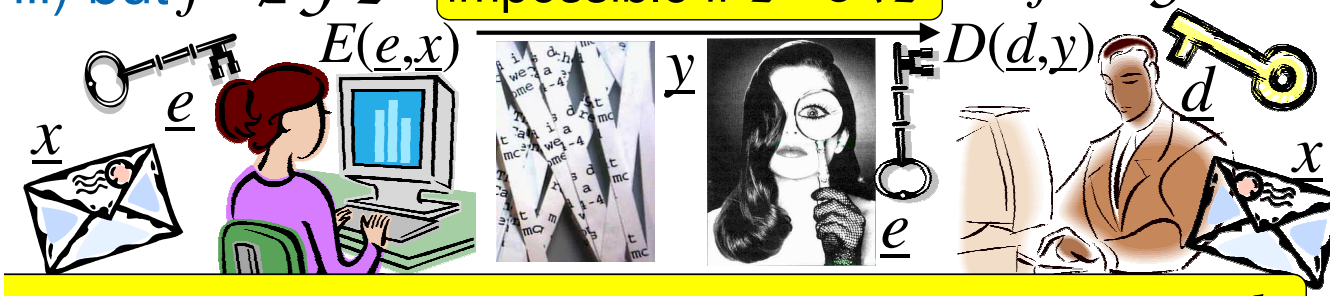
Call $f:\mathbb{N}\to\mathbb{N}$ a one-way function if

RSA

i) injective and $\ell(\mathrm{x}(\underline{x})^k \geq \ell(f(\underline{x})) \geq \ell(\underline{x})^{1/k}$ 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 private key $\underline{e}$, decrypt with public key $\underline{d}$.

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

KAIST CS422 M. Ziegler

Definition: Call a *non*determin. **WHILE+** program unambiguous if, for any input x, it has *at most* one accepting computation.

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

$\mathcal{UP}$ = { decision problems accepted by unambiguous polynomial-time nondetermin. **WHILE+** programs}

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

Proof $\Leftarrow$: For one-way f let $L := \{ \langle x,y\rangle \mid \exists z\leq x: f(z)=y \}$
Then $L\in\mathcal{UP}$. If $L\in\mathcal{P}$, then binary search with polynomially many queries would yield $f^{-1}\in\mathcal{FP}$.

$\Rightarrow$: Let $\mathcal{UP}\setminus\mathcal{P} \ni L = \{ x \mid \exists! z : \ell(z)\leq\ell(x)^k, \langle x,z\rangle \in V \}$.
Define $f(\langle x,z\rangle):=2x+1$ for $\langle x,z\rangle\in V$; else $f(\langle x,z\rangle):=2\langle x,z\rangle$
This is one-way!