Public-key Encryption

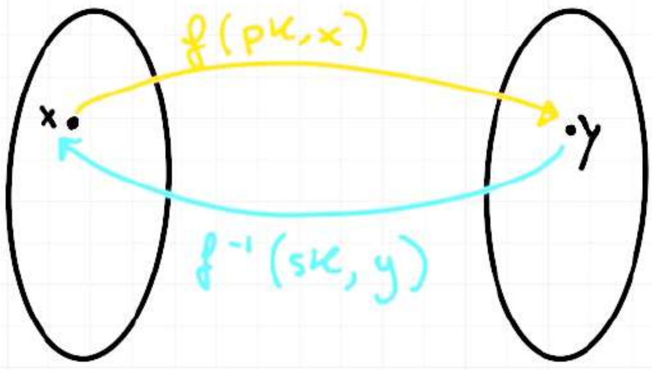
We saw two main definitions for PKE: CPA/CCA security.
Under which assumption can we have CPA/CCA secure PKE?
It is not possible in minicrypt, but it is possible by assuming TRAPDOOR PERMUTATIONS (TDPs), but also assuming FACTORING and DDH.

A triple (Gen, f, f^{-1}) is a TDP if

- $(pk, sk) \leftarrow\$ Gen(1^\lambda)$
- $f(pk, \cdot)$ is an efficiently computable permutation over domain $\mathcal{X}_{pk}$.
- $f^{-1}(sk, y)$ is also efficiently computable such that

$$\forall (pk, sk) \in Gen(1^\lambda), \forall x \in \mathcal{X}_{pk}, \forall \lambda \in \mathbb{N}$$

$$f^{-1}(sk, f(pk, x)) = x$$



Security: hard to invert $f(pk, x)$ on random x without knowing sk.

$$
\begin{array}{ccc}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
 & \xleftarrow{\quad pk \quad} & (pk, sk) \leftarrow \$ \, Gen(1^\lambda) \\
 & \xleftarrow{\quad y = f(pk, x) \quad} & x \leftarrow \$ \, \mathcal{X}_{pk} \\
 & \xrightarrow{\quad x' \quad} & \text{Output } 1 \text{ if } x' = x
\end{array}
$$

Does a TDP trivially imply PKE?

<u>NO</u> because deterministic encryption is never CPA secure.

Here is a fix: Let h be the hard-core predicate associated to f. (Recall: h exists by GL theorem)

This means that $(f(x), h(x)) \approx_c (f(x), b)$ with $x \leftarrow \$ \, \mathcal{X}$, $b \leftarrow \$ \, \{0,1\}$

So I can build

$\Pi = (KGen, Enc, Dec)$ over $\mathcal{M} = \{0,1\}$.

$KGen = Gen(1^\lambda)$ (the one of TDP)

$Enc(pk, m \in \{0,1\}) : (f(pk, r), h(pk, r) \oplus m)$

$r \leftarrow \$ \, \mathcal{X}_{pk}$

$Dec(sk, (c_1, c_2)) : f^{-1}(sk, c_1) = r$

$m = \overset{h(pk,r)}{f}(pk, r) \oplus c_2$ c2 è un bit

<u>THM</u> Π is CPA secure if (Gen, f, f^{-1}) is a TDP.

Proof is left as excercise. Reduction to security of h:

A' $\quad$ ~~A_{CPA}~~ $\quad\quad$ $A(1^\lambda)$ $\quad\quad\quad\quad$ $\mathcal{C}(1^\lambda)$

$\xleftarrow{pk}$ $\quad\quad\quad\quad$ $\xleftarrow{f(pk,r),\, z}$

$(pk, sk) \leftarrow \$\, Gen(1^\lambda)$

$\xrightarrow{0,1}$

$r \leftarrow \$\, \mathcal{X}_{pk}$

$c_1 = f(pk, r)$

$c_2 = z \oplus b$

$z \leftarrow \$\{0,1\}$ or $z = h(pk, r)$

$\hookrightarrow$ can distinguish $GAME^{cpa}_{\pi,\lambda}$ from $HYB^{cpa}_{\pi,\lambda}$ (where $c_1 = f(pk, r)$
$c_2 = z \oplus m_b$ $\;z \leftarrow \$\{0,1\}$

This reduction shows that

$$\forall b \in \{0,1\},\ GAME(\lambda, b) \approx_c HYB(\lambda, b)$$

$$HYB(\lambda, 0) \equiv HYB(\lambda, 1)$$

With this construction, however, we can just encrypt one bit.

EXERCISE: Single-bit CPA-secure PKE implies Multi-bit CPA-secure PKE.

Not very efficient. Let's do better by looking at concrete TDPs. Two examples are

RSA and Rabin's TDP.

Number theory time! Let's look at $\mathbb{Z}_n, \mathbb{Z}_n^*$ with $n = p \cdot q$.
An important ingredient is:

<u>THM</u> $\mathbb{Z}_n$ (or $\mathbb{Z}_n^*$) is ISOMORPHIC to $\mathbb{Z}_p \times \mathbb{Z}_p$

(or $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$) CHINESE REMAINDER THM

This mean that $\exists$ map $\psi : \mathbb{Z}_n^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

$$\forall a \in \mathbb{Z}_n^* \quad \psi(a) = (\underbrace{a_p, a_q}_{(a \bmod p,\ a \bmod q)})$$

It's easy to see $\exists \psi^{-1} : \mathbb{Z}_p^* \times \mathbb{Z}_q^* \to \mathbb{Z}_n^*$

Note: $\psi(a+b) = (a_p + b_p, a_q + b_q)$
$\psi(a \cdot b) = (a_p b_p, a_q b_q)$

Since $\gcd(p,q) = 1$, $\exists x, y$ s.t. $px \cdot qy = 1$

$$\Rightarrow px \equiv 1 \bmod q, \quad qy \equiv 1 \bmod p$$

$$\Rightarrow \psi(px) = (0,1) \quad \psi(qy) = (1,0)$$

$$\Rightarrow \psi^{-1}(\alpha, \beta) = \alpha qy + \beta px$$

$$a_p = \alpha, \ a_q = \beta$$

Look at $f_e(x) = x^e \bmod n$ for $n = p \cdot q$

$\# \mathbb{Z}_n^* = \varphi(n) = (p-1)(q-1)$

So long as $\gcd(e, \varphi(n)) = 1$ we get that $f_e(\cdot)$ is a permutation over $\mathbb{Z}_n^*$, because $\exists d$ s.t. $d \cdot e \equiv 1 \mod \varphi(n)$

d inverso di e

$$\Rightarrow f^{-1}(d, x^e) = (x^e)^d \mod n$$

t multiplo di fi, +1 perché la divisione deve dare 1 di resto

$$= x^{t \cdot \varphi(n) + 1} \mod n \quad \text{by Fermat}$$

$$= x \mod n$$

<u>CONJECTURE</u>: $(\text{GenRSA}, f_e, f_d^{-1})$ is a TDP.

GenRSA(1^λ) outputs $pk = (n, e)$ $\quad d \cdot e = 1 \mod \varphi(n)$

$sk = (n, d)$ $\quad n = p \cdot q$

$f_e(x) = x^e \mod n$ $\quad$ e any value s.t.

$f_d^{-1}(x) = y^d \mod n$ $\quad$ $\gcd(e, \varphi(n)) = 1$

efficient modular exponantiation

(for example, $e = 3$)

Explicitly:

$$\begin{array}{ccc}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
& \xleftarrow{(pk, sk)} & (pk, sk) \leftarrow\$ \text{GenRSA} \\
& \xleftarrow{y = x^e \mod n} & x \leftarrow \mathbb{Z}_n^* \\
& \xrightarrow{x^{-1}} & \text{output } 1 \text{ if } x' = x
\end{array}$$

RSA $\Rightarrow$ Factoring. If we can factor $n = pq$, we can compute

$\varphi(n)$, thus we can compute d and invert the above y.

However, Factoring $\not\Rightarrow$ RSA ? we don't know non sappiamo solo che per rompere rsa bisogna fattorizzzare in modo efficiente

RSA $\Rightarrow$ TDPs $\Rightarrow$ PKE

Rivest, Shamir and Adleman:

$$\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$$

$\hat{m}$ is the padded message

$$\text{KGen} = \text{GenRSA}$$
$$\text{Enc}(pk = (n,e), m) = (\underbrace{\hat{m}}_{(r \| m)})^e \bmod n \qquad r \leftarrow\$ \{0,1\}^\ell$$

$$\text{Dec}(sk = (n,d), c) = c^d \bmod n = \hat{m}$$
$$= m \| \cancel{r} = m$$

Padding is standardized under PKCS # 1,5

$$\hat{m} = 0 \| 1 \| \underbrace{r}_{\geq 8 \text{ bytes}} \| m$$

What about security? Obviously insecure for $\ell \in O(\log \lambda)$.
On the other extreme, CPA secure under RSA if $m \in \{0,1\}$.
Elsewhere: not known ¯_(͡° ͜ʖ ͡°)_/¯

Also, it's not CCA secure (Famous attack in the 90's)

Plan: 1) TDP from FACTORING $\Rightarrow$ PKE from FACTORING

2) CPA/CCA PKE from DDH
(efficient)