Symmetric vs. public-key crypto

Symmetric keys

- Common key k (secret)
- Both for encryption and decryption
- Secure channel without trusted third party

Public key cryptography

- pk, sk pair of keys (public, secret)
- pk at sender, sk at receiver
- distribute keys:
  - pk publicly sent (through authenticated channel)
  - pk broadcast, independent of sender
- multiple senders – one receiver
- 2-3 orders of magnitude slower :(

Definiition of public key scheme

Definition

A public key scheme is a triple $\Pi = (Gen, Enc, Dec)$ *with:*

- Gen, *the key generation, a prob. algorithm that has* 1^n *as input (security param.) and* (pk, sk) *as output (key pair). The public key is* pk, *the secret key is* sk, *and* $|pk|, |sk| \geq n$
- Enc, *the encryption, a PPT algo. with* pk *and message* $m \in \mathcal{M}$) *as inputs and* $c \in \mathcal{C}$, $c := Enc_{pk}(m)$ *as output (ciphertext)*
- Dec, *the decryption a deterministic algo. with* sk *and* $c \in \mathcal{C}$ *as inputs. The output is an element of* $\mathcal{M}$, $Dec_{sk}(c)$.

Properties of public key scheme

Correctness

We trivially need $\forall n, \forall pk, sk$ and $\forall m \in \mathcal{M}$, that

$$Dec_{sk}Enc_{pk}(m) = m.$$

.

Attacks against public key schemes

Definition (indistinguishability experiment with eavesdropping $PubK^{eav}_{\mathcal{A},\Pi}(n)$)

1. $Gen(1^n) = (pk, sk)$
2. *The adversary $\mathcal{A}$ issues messages $m_0, m_1 \in \mathcal{M}$ on input pk, where $|m_0| = |m_1|$.*
3. $k = Gen(1^n), b \in_R \{0, 1\} : c = Enc_{pk}(m_b)$ *given to* $\mathcal{A}$
4. $\mathcal{A}$ *issues* $b' \in \{0, 1\}$
5. $PubK^{eav}_{\mathcal{A},\Pi}(n) = 1$, *if* $b = b'$, *otherwise 0.*

Attacks against public key schemes

Definition

A scheme $\Pi = (Gen, Enc, Dec)$ *is secure agains one eavesdropping if any PPT adversary* $\forall \mathcal{A}$, $\exists e(.)$ *negligible s.t.*

$$P(PubK^{eav}_{\mathcal{A},\Pi}(n) = 1) \leq \frac{1}{2} + e(n).$$

Attacks against public key schemes

Definition (CPA indistinguishability experiment $PubK^{cpa}_{\mathcal{A},\Pi}(n)$)

1. $Gen(1^n) = (pk, sk)$
2. *The adversary $\mathcal{A}$ has oracle access to $Enc_{pk}(.)$ for pk, then issues m_0, m_1, with $|m_0| = |m_1|$*
3. $b \in_R \{0, 1\} : c = Enc_{pk}(m_b)$ *given to $\mathcal{A}$*
4. *$\mathcal{A}$ has renewed oracle access to $Enc_{pk}(.)$. Then issues $b' \in \{0, 1\}$*
5. $PubK^{cpa}_{\mathcal{A},\Pi}(n) = 1$, *if $b = b'$, otherwise 0.*

Attacks against public key schemes

Definition

A scheme $\Pi = (Gen, Enc, Dec)$ *is CPA-secure if for any PPT adversary* $\forall \mathcal{A}$, $\exists e(.)$ *negligible s.t.*

$$P(PubK^{cpa}_{\mathcal{A},\Pi}(n) = 1) \leq \frac{1}{2} + e(n).$$

Attacks against public key schemes

Definition (indistinguishability experiment with multiple eavesdroppings $PubK^{meav}_{\mathcal{A},\Pi}(n)$)

Slight modification of definition

1. *Adversary $\mathcal{A}$ issues* $M_0 = (m_{01}, \ldots, m_{0t}), M_1 = (m_{11}, \ldots, m_{1t})$ *sequences,* $\forall i : |m_{0i}| = |m_{1i}|$
2. $b \in_R \{0, 1\} : C = (c_1, \ldots, c_t) : c_i = Enc_{pk}(m_{bi})$ *is given to* $\mathcal{A}$

Attacks against public key schemes

Theorem

If Π is secure against one eavesdropping $\Rightarrow$ CPA-security folllows

Theorem

If Π is secure against one eavesdropping $\Rightarrow$ also secure against multiple eavesdroppings

Theorem

$\nexists\Pi$ perfectly secure scheme (i.e. $\forall\mathcal{A} : PubK^{eav}_{\mathcal{A},\Pi}(n) = 1/2$)

Number theory for cypto

Euler's totient function φ

- $\varphi(n) = |\{k : 1 \leq k \leq n, (k,n) = 1\}|$
- p prime: $\varphi(p) = p - 1, \varphi(p^m) = p^m - p^{m-1}$
- $\varphi(nm) = \varphi(n)\varphi(m)$, ha $(n,m) = 1$

Theorem (Euler–Fermat)

$\forall a : 1 \leq a \leq n, (a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \mod n.$

Number theory for cypto

Theorem (Prime number theorem)

For $x > 0$ let $\pi(x)$ denote the number of primes up to x. We have $\pi(x) \sim \frac{x}{\log x}$

Corollary

$\exists c > 0 \forall n > 1$: *Number of n-bit primes roughly $c \cdot 2^{n-1}/n$.*

- n^2/c random picks will result in at least one prime with prob. $1 - 1/e^n$
- 2002: DPT primality test
- practice: PPT test
- e.g. Miller-Rabin

Textbook RSA

Textbook RSA

Gen
- For input 1^n, choose primes p, q with n-bits. Set $N = pq$
- Let $e \in \{2, \ldots, N-1\} : (e, \varphi(N)) = 1$
- Let $d \in \{2, \ldots, N-1\} : ed \equiv 1 \mod \varphi(N)$
- $pk = (N, e), sk = (p, q, d)$

Enc For message $m \in \mathbb{Z}_N^*$ and private key pk, let $c \equiv m^e \mod N$

Dec For ciphertext $c \in \mathbb{Z}_N^*$ and secret key sk, let $m \equiv c^d \mod N$

Seciruty of textbook RSA

Textbook RSA

Gen
- $N = pq, ed \equiv 1 \mod \varphi(N)$
- $pk = (N, e), sk = (p, q, d)$

Enc For $m \in \mathbb{Z}_N^*$ and pk, $c \equiv m^e \mod N$

Dec For $c \in \mathbb{Z}_N^*$ and sk, $m \equiv c^d \mod N$

Security

- correctness: $(x^e)^d) = x^{ed} \equiv x^{ed \bmod \varphi(N)} \equiv x^1 = x$
- Enc DPT $\Rightarrow$ no security unless randomization added

RSA

Factorization problem

For random RSA modulus input N, find $p, q : N = pq$.

RSA problem

For random RSA instance N, e, c, find $m : m^e \equiv c \mod N$.

Statement

Factoring tractable $\Rightarrow$ *RSA tractable. Note:* $\Leftarrow$ *only conjectured.*

RSA

Properties

- Rivest, Shamir, Adleman '76
- p, q 1024-bit Sophie-Germain primes ($2p + 1$ is also prime)
- $e = 2^{16} + 1$ (prím)
- PPP encryption: $m' = (r||m)$ with r fixed length random

Theorem

If RSA problem difficult $\Rightarrow$ randomized RSA is CPA-secure