Lecture 14

1 Encryption

Figure 1: Public/private Key Encryption

Do we actually need a secret shared between Alice and Bob? D must take as its input some secret unknown to Eve, and perhaps known to Alice? The truth is that the secret doesn't have to be known to Alice.

Main idea is to use two different keys:

tk - private key (used for decryption)

pk - public key (used for encryption, made public)

2 Assymetric Encryption Schemes

Definition 1 An asymmetric encryption scheme is defined by, (G, E, D), with signatures

$G : () \to \mathcal{PK} \times \mathcal{TK}$

$E : \mathcal{PK} \times \mathcal{M} \to \mathcal{C}$

$D : \mathcal{TK} \times \mathcal{C} \to \mathcal{M} \cup \perp$

where (G, E, D) satisfy the following requirements:

1. $D_{tk}(Epk(m)) = m \ \forall \ (pk, tk) \leftarrow G()$
2. G, E, D must be implementable by efficient algorithms (polynomical-time implementable)
3. IND-CPA:

$$AdvA = |\Pr[A^{E_{pk}(\cdot)}(pk) = 1] - \Pr[A^{E_{pk}(\$(\cdot))}(pk) = 1]|$$

Assumption: E is a randomized encryption algorithm. If E wasn't randomized, an adversary could simply run its own copy of E and compare the answers.

4. IND-CCA2:

$$AdvA = |\Pr[A^{E_{pk}(\cdot),D_{tk}(\cdot)}(pk) = 1] - \Pr[A^{E_{pk}(\$(\cdot)),D_{tk}(\cdot)}(pk) = 1]|$$

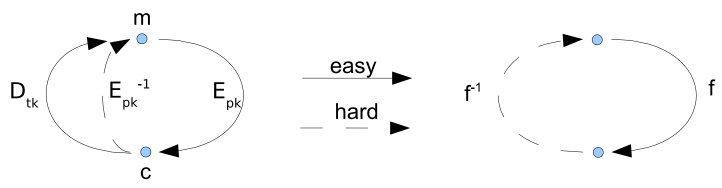

Figure 2: Primitive: Trapdoor One-way Permutation

Example 1 (One way function) Given p, q primes, define $f(p, q) = pq$. Although f^{-1} requires fast factorization and is hard to compute, there is shortcut trapdoor. So f alone is insufficient for a candidate trapdoor one-way permutation.

Ultimately, we want an F such that:

1. $(pk, tk) \leftarrow G()$
2. $F_{pk} : \mathcal{X} \to \mathcal{X}$ and F is bijective
3. $F_{tk}^{-1} : \mathcal{X} \to \mathcal{X}$ and ${F^{-1}}_{tk}(F_{pk}(x)) = x \;\forall\; x \in \mathcal{X}$

Definition 2 (Trapdoor One-way Permutation) F is a (t, ϵ) is trapdoor one-way permutation if

$$\Pr[(pk, tk) \leftarrow G(); x \xleftarrow{\$} \mathcal{X}; A(pk, F_{pk}(x)) = x] \leq \epsilon \;\forall\; A \text{ running in time } t$$

In other words, we can think of G as returning two functions (i.e. $(f, f^{-1}) \leftarrow G()$). With respect to an adversary A, these two functions have the property that

$$\Pr[x \xleftarrow{\$} \mathcal{X}; A(f, f(x)) = x] \leq \epsilon$$

3 RSA

RSA operates by picking a public key, $pk = n = pq$, where both p and q are primes. The private key is then $tk = (p, q)$.

The trapdoor function f is a function over a group $\mathcal{X} = (\mathbb{Z}/n\mathbb{Z})^*$, i.e. $f : \mathcal{X} \to \mathcal{X}$. RSA defines $f(x) = x^3 \; mod \; n$. The underlying implication is that f^{-1} must be hard to compute without the corresponding pair of primes and easy to compute when the primes are known, thus enabling the trapdoor mechanism.

We now illustrate the trapdoor mechanism for RSA's f. The inverse function f^{-1}, is $f^{-1}(y) = y^d \; mod \; n$, where $d = 3^{-1} \; mod \; \varphi(n)$, $\varphi(n)$ is the totient function and 3^{-1} is the multiplicative inverse of 3. The totient function $\varphi(n)$, also called Euler's totient function, is defined as the number of positive integers $\leq n$ that are relatively prime to (i.e., do not contain any factor in common with) n, where 1 is counted as being relatively prime to all numbers. A useful property of the totient function is that $\varphi(n) = \varphi(p) \times \varphi(q) = (p-1)(q-1)$ when $n = p \times q$ and p, q are both prime.

Since d is defined in terms of multiplicative inverse, we can easily compute

$$f^{-1}(f(x)) = x^{3d} \ mod \ n = x \ mod \ n = x$$

but without knowing d or prime factorization of n we are stuck.

Conjecture 1 (RSA Assumption)

$$\Pr[A(n, x^3 \ mod \ n) = x] \leq \text{"negligible amount"}$$

Existence of a trapdoor one-way permutation does not give rise to an encryption scheme. Why? For one, f deterministic, and we have established that deterministic encryption is inherently insecure.

4 Chinese Remainder Theorem

RSA uses $x^3 \ mod \ n$, so why not $x^2 \ mod \ n$? What would the inverse function for f be?

Theorem 2 (Chinese Remainder Theorem (small part))
There is a congruence between the sets $(\mathbb{Z}/n\mathbb{Z})$ and $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ which is computed as follows:

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \cong & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ x & \mapsto & (x \ mod \ p, x \ mod \ q) \\ a + \alpha(b-a) \ mod \ n & \leftarrow & (a, b) \end{array}$$

where $\alpha = 0(\ mod \ p)$ and $\alpha = 1(\ mod \ q)$.

Definition 3 An element $x \in \mathbb{Z}_n$ is said to be a quadratic residue $\pmod n$ if there exists an element $y \in \mathbb{Z}_n$ such that $x = y \cdot y \pmod n$. If so, y is said to be a square root of x (mod n).

It is easy to see that

$$\begin{array}{ccc} QR_p & \subseteq & (\mathbb{Z}/p\mathbb{Z})^* \\ \{g^2, g^4, g^8, \ldots, 1\} & \subseteq & \{g, g^2, g^3, \ldots, 1\} \end{array}$$

for a generator g and $(\mathbb{Z}/p\mathbb{Z})$ is known to be cyclic for prime p.

Lemma 3 (Bijective Square Roots)
If $p \equiv 3(\ mod \ 4)$, $2 \mid p-1$, $4 \not| p-1$, then

$$\{g^4, g^8, g^12, \ldots, g^{p-3}, g^{p+1}, gp+5, \ldots, g^{2p-2} = 1\} = QR_p$$

The square root function $\sqrt{\ }$, $\sqrt{\ } : QR_p \to QR_p$ is now bijective for prime p chosen as described above. Similarly, if q is chosen the same way, then $\sqrt{\ } : QR_q \to QR_q$ is also bijective.

We can now partition groups $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/q\mathbb{Z}$ as follows.

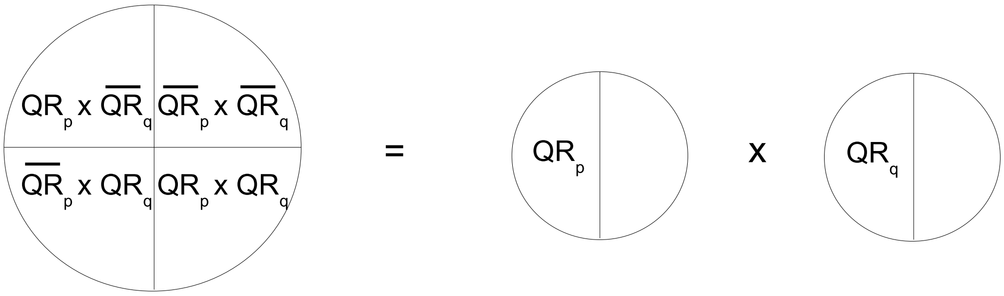

Figure 3: Partitioning $\mathbb{Z}/n\mathbb{Z}$

$$\begin{array}{rcl}
x & \mapsto & (a,b) \\
x^2 & \leftarrow & (a^2,b^2) \\
x & \mapsto & (a,b) \\
1 & \leftarrow & (a^2,b^2) = (1,1)
\end{array}$$

Likewise, we can define the four roots of a pair (a,b):

$$\begin{array}{rcl}
x & : & (a,b) \\
1 & \leftarrow & (1,1) \\
\omega & \leftarrow & (1,q-1) \\
-\omega & \leftarrow & (p-1,1) \\
-1 & \leftarrow & (p-1,q-1)
\end{array}$$

By partition of the sets shown above, the function $\sqrt{\ } : (\mathbb{Z}/n\mathbb{Z})^* \to \sqrt{\ }_n$ is a 4-to-1 function. Conversely, $\sqrt{\ } : \sqrt{\ }_n \to \sqrt{\ }_n$ is a 1-to-1 function as long as both $p = 3 \pmod 4$ and $q = 3 \pmod 4$ prime. Finally, we can define f and its inverse f^{-1}.

Definition 4 (Rabin's One-way Trapdoor Function) Pick $p, q = 3 \pmod 4$ prime, and $n = pq$.

$$\begin{array}{rcl}
f(x) & = & x^2 \; mod \; n \\
f^{-1}(y) & = & CRT(\sqrt{y \; mod \; p}, \sqrt{y \; mod \; q})
\end{array}$$