Public Key Encryption

Thursday, October 12, 2017 12:28 PM

Conceptually Simple Public Key Encryption using Diffie-Hellman Key Exchange

A

Alice ———— Bob

$a \in \mathbb{Z}_p$ $\qquad$ $b \xleftarrow{\$} \mathbb{Z}_p$

$A = g^a$ $\qquad$ $B = g^b$

$\leftarrow$ publish B

$\underline{\underline{k}} := H(B^a)$ $\qquad$ $\underline{\underline{k}} := H(A^b)$

$(\underline{\underline{A}}, \underline{Enc_k(m)}) \rightarrow$

RSA Encryption

$p \xleftarrow{\$} \Pi_\lambda \leftarrow$ set of all primes up to 2^λ

$q \xleftarrow{\$} \Pi_\lambda$

public $\rightarrow$ $N = \underline{pq} \leftarrow$ secrets

RSA modulus

work in the group $\mathbb{Z}_{\underline{N}}^*$

Definition:

Euler's totient function:

$\varphi(n)$ the number of integers $< n$ relatively prime to n

Fact: $\varphi(pq) = \underline{(p-1)(q-1)}$ when p and q are prime

Not coprime so it must be divisible by p or divisible by q

Bob's pub key

Alice (N):

$e = 65,537$

$2^{16}+1$

$\mathrm{Enc}_N(m)$:

$c := m^e \bmod N$

secret key (random primes p and q)

Bob (p,q):

$\varphi(N) = (p-1)(q-1)$ $\gcd(e, \varphi(N)) = 1$

$d =$ solve $d \cdot e = 1 \bmod \varphi(N)$

Extended Euclidean algorithm

$\mathrm{Dec}(c)$:

output $m' := c^d \bmod N$

Correctness property $\mathrm{Dec}_d(\mathrm{Enc}_N(m)) = m$

(not needed)

Euler's Theorem: If a and N are relatively prime, then $a^{\varphi(N)} = 1 \bmod N$

Strong RSA assumption:

Given (N, e, y)

$N = pq$ for random primes p, q,

$\gcd(e, \varphi(N)) = 1$, and $y \xleftarrow{\$} \mathbb{Z}_N^*$

then it's hard to compute X so that $X^e = y \bmod N$

$\forall A, \Pr\left[p,q \xleftarrow{\$} \Pi_\lambda, N = pq, e = 65537, X \leftarrow A(N,e,y) : X^e = y \bmod N\right] \leq \mathrm{negl}$
$y \xleftarrow{\$} \mathbb{Z}_N$

Claim: $f_{N,e}(x) = x^e \bmod N$ is a OWF

Claim: RSA function is a permutation on $\mathbb{Z}_N^*$

Let d be the inverse of e, so $d \cdot e = 1 \pmod{\varphi(N)}$

Then $f^{-1}_{d,N,e}(y) = y^d \bmod N$

for some c

$$(x^e)^d \bmod N = x^{c\varphi(n)+1} \bmod N \quad (\text{by } \checkmark)$$

$$= x(x^{c\varphi(n)}) = x \quad (\text{by Euler's theorem})$$

$$x^{\varphi(N)} = 1$$

? needs x relatively prime to $\varphi(N)$

Syntax of Public Key Encryption

(Gen, Enc, Dec)

- $\text{Gen}(1^\lambda) \rightarrow$ outputs (sk, pk)
- $\text{Enc}_{pk}(m) \rightarrow$ ciphertext c
- $\text{Dec}_{sk}(c) \rightarrow m$ the message

Security:

$$\forall m_0, m_1 \quad \{(pk, sk) \leftarrow \text{Gen}(1^\lambda) : (\underbrace{pk}_{\substack{g^a \\ \text{group element}}}, \underbrace{\text{Enc}_{pk}(m_0)}_{\substack{(g^b,\ g^{ab}m) \\ (\text{group element, group element})}})\}$$

$$\approx \{(pk, sk) \leftarrow \text{Gen}(1^\lambda) : (pk, \text{Enc}_{pk}(m_1))\}$$

- Useful in simulation proofs.
- Problem: RSA encryption naively work.

  $pk = (N, e)$, $\quad sk = (p, q, \varphi(N), d)$

  $\text{Enc}_{pk}(m) = m^e \bmod n$, $\quad \text{Dec}_{sk}(c) = c^d \bmod n$
- Can encrypt 1 bit using hardcore predicate for RSA as OWF

  (see 3.10.1)

El Gamal Encryption:

Let $G = \langle g \rangle$ be a DDH group, $|G| = p$, prime

- $\text{Gen}(1^\lambda)$: $pk = A = g^a$, $a \xleftarrow{\$} \mathbb{Z}_p$ is sk
- $\text{Enc}_A(m)$: $b \xleftarrow{\$} \mathbb{Z}_p$

  output $c = (g^b, \underbrace{A^b \cdot m}_{})$
- $\text{Dec}(c)$ = parse c as (B, c')

output $\underline{m'} := C'/B^a$

Correctness: $m' = C'/B^a = (A^b \cdot m)/(B^a)$

$= ((g^a)^b \cdot m)/((g^b)^a)$

$= m$

Security:

Given m_0, m_1, $\mathcal{A}$ where $\underline{\mathcal{A}}$ breaks Message Security on m_0, m_1,

Construct $\underline{\mathcal{A}'}(A, B, C)$ that distinguishes $\underline{DDH}$

$0 \rightarrow \{a \xleftarrow{\$} \mathbb{Z}_p, b \xleftarrow{\$} \mathbb{Z}_p ; (g^a, g^b, g^{ab})\}$

$1 \rightarrow$ from $\{a \xleftarrow{\$} \mathbb{Z}_p, b \xleftarrow{\$} \mathbb{Z}_p, r \xleftarrow{\$} \mathbb{Z}_p : (g^a, g^b, \underline{g^r})\}$

$\mathcal{A}'(A, B, C)$:

call $v_0 \leftarrow \underline{\mathcal{A}}(pk = A, c = (B, \underline{C \cdot m_0}))$

call $v_1 \leftarrow \underline{\mathcal{A}}(pk = A, c = (B, \underline{C \cdot m_1}))$

output 1 if $\underline{v_0 \neq v_1}$.

$$\boxed{\left| \Pr[\mathcal{A}^{(m_0)} = 1] - \Pr[\mathcal{A}^{(m_1)} = 1] \right| = \text{nonnegl}}$$

Why? $\underline{\text{Case 0}}$: $\mathcal{A}$ distinguishes Enc(m_0) from Enc(m_1) with prob $\frac{1}{2} + \varepsilon$ then

$v_0 \neq v_1$ w/ prob $\underline{\frac{1}{2} + \varepsilon}$

Case 1: $v_0 = v_1$ w/ exactly $\frac{1}{2}$ $\underline{\text{probability}}$.