THE RABIN-WILLIAMS PKC

1. Description of Rabin-Williams

Public-key encryption scheme provably equivalent to integer factorization (Rabin, Williams 1980).

Modification of Rabin's scheme (similar to RSA using $e = 2$) with unique decryption.

Lemma 1.1. *Let $n = pq$ with $p \equiv q \equiv -1 \pmod 4$. If $\left(\frac{M}{n}\right) = 1$, then*

$$M^{\phi(n)/4} \equiv \pm 1 \pmod n$$

Proof. $\left(\frac{M}{pq}\right) = 1 \longrightarrow \left(\frac{M}{p}\right) = \left(\frac{M}{q}\right)$. If $\left(\frac{M}{p}\right) = 1$, then

$$M^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$M^{\frac{p-1}{2}\frac{q-1}{2}} \equiv 1 \pmod p\ .$$

Similarly,

$$M^{\frac{q-1}{2}\frac{p-1}{2}} \equiv 1 \pmod q$$

and by the CRT we have $M^{\phi(n)/4} \equiv 1 \pmod n$.

If $\left(\frac{M}{p}\right) = -1$, then we use the fact that $(-1)^{(p-1)/2} \equiv -1 \pmod p$ when $p \equiv -1 \pmod 4$ to argue that $M^{\phi(n)/4} \equiv -1 \pmod n$. □

1.1. Key Generation.

Select large primes p, q with $p \equiv 3 \pmod 8$, $q \equiv 7 \pmod 8$, and put $n = pq$.

Select at random e such that $1 < e < n$ and $\gcd(e, \phi(n)) = 1$.

Solve $ed \equiv m \pmod{\phi(n)}$ where $m = (\phi(n)/4 + 1)/2$.

Public key: $\{n, e\}$ Private key: $\{d\}$

1.2. Encryption and Decryption.

Define $\mathcal{M} = \{M \mid (2(2M+1) < n \text{ and } \left(\frac{2M+1}{n}\right) = -1) \text{ or } (4(2M+1) < n \text{ and } \left(\frac{2M+1}{n}\right) = 1)\}$.

Theorem 1.2. *$|\mathcal{M}| = 3/16\phi(n) - t$ and $t < 1/2\sqrt{n}\log n + 5/4$ (i.e., $|\mathcal{M}| \in O(n)$).*

For $M \in \mathcal{M}$ define:

$$E_1(M) = \begin{cases} 4(2M+1) & \text{if } \left(\frac{2M+1}{n}\right) = 1 \\ 2(2M+1) & \text{if } \left(\frac{2M+1}{n}\right) = -1 \end{cases} \quad \left(\text{note } \left(\frac{E_1(M)}{n}\right) = 1\right)$$

$$E_2(N) \equiv N^{2e} \pmod n \quad (0 < E_2(N) < n \text{ and } N \in \mathbb{Z}),$$

$$D_2(K) \equiv K^d \pmod n \quad (0 < D_2(K) < n),$$

$$D_1(L) = \begin{cases} (L/4-1)/2 & \text{if } L \equiv 0 \pmod 4 \\ ((n-L)/4-1)/2 & \text{if } L \equiv 1 \pmod 4 \\ (L/2-1)/2 & \text{if } L \equiv 2 \pmod 4 \\ ((n-L)/2-1)/2 & \text{if } L \equiv 3 \pmod 4 \end{cases}$$

To encrypt $M \in \mathcal{M}$, the sender computes $C = E_2(E_1(M))$.

To decrypt C, the receiver computes $D_1(D_2(C)) = M$.

2. Proof of Equivalence to Factoring

Theorem 2.1. *If $M \in \mathcal{M}$ then $D_1 D_2 E_2 E_1(M) = M$.*

Proof. We have:

$$N = E_1(M) \quad \text{with } 2 \,|\, N,\ 0 < N < n, \text{ and } \left(\frac{N}{n}\right) = 1$$
$$L = D_2E_2(N) \equiv N^{2ed} \equiv N^{2m} \equiv N^{\phi(n)/4+1} \equiv \pm N \pmod n \quad \text{with } 0 < L < n \text{ and } n \equiv 1 \pmod 4$$

Thus, if L is even, then $L = N$ and if L is odd, then $L = n - N$.
If $L \equiv 0 \pmod 4$, then $(2M + 1) = N/4 = L/4 \longrightarrow M = (L/4 - 1)/2 = D_1(L)$.
If $L \equiv 1 \pmod 4$, then $2M + 1 = (n - L)/4 \longrightarrow M = ((n - L)/4 - 1)/2 = D_1(L)$.
If $L \equiv 2 \pmod 4$, then $2M + 1 = L/2 \longrightarrow M = (L/2 - 1)/2 = D_1(L)$
If $L \equiv 3 \pmod 4$, then $2M + 1 = (n - L)/2 \longrightarrow M = D_1(L)$. □

We will now show that breaking the encryption scheme is equivalent in difficulty to factoring n.

Lemma 2.2. *If n is given as above, then for any $X \in \mathbb{Z}$ there exists $Y \in \mathbb{Z}$ such that $X^2 \equiv Y^2 \pmod n$ and $\left(\frac{Y}{n}\right) = -\left(\frac{X}{n}\right)$.*

Proof. $\left(\frac{-X}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{X}{p}\right) = -\left(\frac{X}{p}\right)$. Let

$$Y \equiv -X \pmod p, \quad Y \equiv X \pmod q\ .$$

Then $Y^2 \equiv X^2 \pmod n$ and

$$\left(\frac{Y}{n}\right) = \left(\frac{Y}{p}\right)\left(\frac{Y}{q}\right) = \left(\frac{-X}{p}\right)\left(\frac{X}{q}\right) = -\left(\frac{X}{n}\right)\ .$$

□

Lemma 2.3. *If $K = E(M)$ (here $E = E_2E_1$), then there exists X_1, X_2 such that $X_1 \neq X_2$, $0 < X_1, X_2 < n$, $X_1^2 \equiv X_2^2 \equiv K \pmod n$ and $\left(\frac{X_1}{n}\right) = \left(\frac{X_2}{n}\right) = -1$.*

Proof. Let $N = E_1(M)$ and $Y \equiv N^e \pmod n$. We have $K \equiv (N^e)^2 \equiv Y^2 \pmod n$ and since $\left(\frac{N}{n}\right) = 1 \longrightarrow \left(\frac{Y}{n}\right) = 1$. By Lemma 2.2 there exists an X such that $X^2 \equiv Y^2 \equiv K \pmod n$ and $\left(\frac{X}{n}\right) = -1$. Let $X_1 \equiv X \pmod n$, $0 < X_1 < n$, and $X_2 = n - X_1$. □

Put $\mathcal{X} = \{X \mid X^2 \equiv E(M) \pmod n, M \in \mathcal{M}, \left(\frac{X}{n}\right) = -1, 0 < X < n\}$. Then $|X| \geq 2|\mathcal{M}|$ by Lemma 2.3. If we select at random a value of X such that $\left(\frac{X}{n}\right) = -1$ and $0 < X < n$ (there are $\phi(n)/2$ such X values) then the probability that there exists an $M \in \mathcal{M}$ such that $X^2 \equiv E(M) \pmod n$ is about $3/4$.

If F is an algorithm which decrypts $1/k$ of all possible ciphertexts, then we see that we can select at random a value of X $(0 < X < n)$ with $\left(\frac{X}{n}\right) = -1$ such that $E(M) \equiv K \equiv X^2 \pmod n$ for some $M \in \mathcal{M}$ and $F(K) = M$ with probability about $\frac{3}{4k}$. We expect to conduct about $4k/3$ trials before such an example is found. Put $Y \equiv E_1(M)^e \equiv E_1(F(K))^e \pmod n$. Then

$$Y^2 \equiv X^2 \pmod n \text{ and } \left(\frac{Y}{n}\right) = 1, \left(\frac{X}{n}\right) = -1$$

and $n = pq \,|\, X^2 - Y^2 \longrightarrow pq \,|\, (X - Y)(X + Y)$. Now:

- If $pq \,|\, X - Y$, then $X \equiv Y \pmod{pq}$, and $\left(\frac{X}{n}\right) = \left(\frac{Y}{n}\right)$, a contradiction.
- If $pq \,|\, X + Y$, then $X \equiv -Y \pmod{pq}$, and $\left(\frac{X}{n}\right) = \left(\frac{-Y}{n}\right) = \left(\frac{Y}{n}\right)$, a contradiction.

Hence, $\gcd(X - Y, n) = p, q$, i.e., we can factor n.