Modern Cryptography

1. The opponent knows the system being used
2. The opponent has access to any amount of corresponding plaintext-ciphertext pairs
3. The opponent has access to the key used in the encrypting transformation $E_k(M) = C$.
4. Security is to be achieved by the opponent not being able to construct the decrypting transformation $D_k(C) = M$.

   A map E_k is said to be a *trapdoor function* if the construction of the inverse map, D_k, is of such theoretical complexity as to make it inaccessible to our present day computational tools.

> NOTE: A trapdoor function may be so today... but may not be so tomorrow!!

The RSA System

1. Choose p and q primes and let $m = pq$
2. Message space: $\{1, 2, \ldots, m-1\}$.
3. Key space: $\{e \mid 1 \le e \le \phi(m), gcd(e, \phi(m)) = 1\}$
4. Encrypting transformation

$$\boxed{C = E_e(M) = M^e \bmod m}$$

5. Decrypting transformation

$$\boxed{M = D_d(C) = C^d \bmod m}$$

where $ed \equiv 1 \bmod \phi(m)$

$\boxed{m,\ e \text{ public}}$ $\boxed{p,\ q,\ d \text{ private}}$

An RSA Example

1. Choose p and q

$$\boxed{p = 1873} \ \boxed{q = 131} \rightarrow \boxed{m = 245,363}$$

2. Select message

$$\boxed{M = 2905}$$

3. Select encrypting exponent

$$\boxed{e = 323}$$

4. Encrypt message

$$\boxed{C = M^e = 2905^{323} \bmod 245{,}363 = 13{,}388}$$

5. Compute decrypting exponent

$$\boxed{ed = 1 \bmod \phi(m)} \rightarrow \boxed{d = 148,247}$$

6. Decrypt message

$$\boxed{C^d = 13,388^{148{,}247} \bmod 245{,}363 = 2905}$$

RSA: Why it works

How do we know that

$$C^d = M^{ed} = M \mod m$$

when $ed = 1 \bmod \phi(m)$?

Recall

Theorem 1 (Euler-Fermat) *If a and m are relatively prime then*

$$a^{\phi(m)} \equiv 1 \quad mod \quad m.$$

What if M and m are not relatively prime?

Theorem 2 (Euler-Fermat for RSA) *If $m = pq$ where p and q are primes then for all integers a and k we have*

$$a^{1+k\phi(m)} \equiv a \quad mod \quad m$$

Proof of Theorem 2

Assume $gcd(a, m) = p$.

$$\gcd(a, m) = p \Rightarrow a = xp \text{ for some } x$$

Therefore

$$\begin{aligned} \gcd(xp, pq) = p \;&\Rightarrow\; \gcd(x, q) = 1 \\ &\Rightarrow\; \gcd(a, q) = 1 \end{aligned}$$

Euler-Fermat yields

$$a^{\phi(q)} \equiv 1 \mod q \;\Rightarrow\; a^{q-1} = 1 + h_1 q$$

Raise both sides to the $k(p-1)$ for any k:

$$a^{k(p-1)(q-1)} = a^{k\phi(m)} = 1 + h_2 q$$

Multiply both sides by a:

$$a^{1+k\phi(m)} = a + ah_2 q = a + h_2 xpq \equiv a \mod m$$

Converting Messages into Numbers

The following is one of many possible methods for converting text into numbers. The basic idea is to use letters as the digits of a number written in base 26. Since any resulting N digit number (base 26) must be less than m, we have that

$$m > 26^N - 1 \;\Rightarrow\; N = \lfloor \log_{26} m \rfloor$$

$$\boxed{m = 245,363 \;\Rightarrow\; N = 3}$$

Encrypt the message "THE":

$$\begin{aligned} \text{“T”}26^0 + \text{“H”}26^1 + \text{“E”}26^2 &= 19 + 7 \cdot 26 + 4 \cdot 26^2 \\ &= 2905 \end{aligned}$$

$$\begin{aligned} 2905^{323} &= 13,388 \mod m \\ &= 24 + 514 \cdot 26 \\ &= 24 + (20 + 19 \cdot 26) \cdot 26 \\ &= 24 + 20 \cdot 26 + 19 \cdot 26^2 + 0 \cdot 26^3 \\ &= \text{“Y”}26^0 + \text{“U”}26^1 + \text{“T”}26^2 + \text{“A”}26^3 \end{aligned}$$

NOTE: Use $N+1$ digits for the ciphertext since some values of $C = M^e$ are on the interval $[26^N, m-1]$.

An Observation

If $m = pq$, with p and q distincts primes, then

$$\phi(m) = (p-1)\,(q-1).$$

It is noteworthy that in this case, we can reconstruct the factorization of m from the knowledge of the value $\phi(m)$.

More precisely, we have

$$\begin{aligned}\phi(m) &= (p-1)(q-1) \\ &= pq - p - q + 1 \\ &= m - (p+q) + 1,\end{aligned}$$

or equivalently,

$$m + 1 - \phi(m) = p + q.$$

Therefore the roots of the polynomial

$$\begin{aligned}x^2 - (m+1-\phi(m))x + m &= x^2 - (p+q)x + pq \\ &= (x-p)(x-q)\end{aligned}$$

are exactly p and q.

Another Observation

Assuming that $m = pq$, the following equation

$$x^2 = 1 \mod m$$

has exactly 4 solutions. They can be found using the Chinese Remainder Theorem applied to each of the following systems of equations

$x = 1 \bmod p$ $x = 1 \bmod q$	$x = 1 \bmod p$ $x = -1 \bmod q$
$x = -1 \bmod p$ $x = 1 \bmod q$	$x = -1 \bmod p$ $x = -1 \bmod q$

Clearly, two of these solutions are $x = \pm 1$, while the other two are $x = \pm a$ for some a. If we could find a, then

$$\begin{aligned} a^2 = 1 \mod m &\Rightarrow a^2 - 1 = km \\ &\Rightarrow (a-1)(a+1) = km \\ &\Rightarrow m = \gcd(a-1, m) \times \gcd(a+1, m) \end{aligned}$$

Given d, the decrypting exponent, there is a probabilistic method to find a.

To find a nontrivial solution of $x^2 \equiv 1 \bmod m$ (with only the knowledge of d), we proceed as follows:

1. **Choose** k at random between 2 and $m-2$.
2. **Compute** $x := \gcd(k, n)$.
3. **If** $x > 1$ **then** x is a factor of n and it must be equal to p or q, so we are **finished**. Otherwise
4. **Write** $ed - 1 = 2^s r$ with r odd.
5. **Compute** $y := k^r$.
6. **If** $y \equiv 1 \pmod{m}$ **then try again**.
7. **Find** the least j $(0 \leq j \leq s)$ such that $y^{2^j} \equiv 1 \pmod{m}$, and set $x := y^{2^{j-1}}$
8. **If** $x \equiv -1 \pmod{n}$ **then try again**,
9. **Else** $(x+1, n)$ is a factor of n and it must be equal to p or q, so we are **finished**.

Digital Signatures (Needs Improvement)

How can we be sure that when we recieve a message from P_i, that it was actually sent by P_i?
Say Alice selects primes p_1 and q_1 and publishes $n_1 = p_1q_1$ and e_1.
Say Bob selects primes p_2 and q_2 and publishes $n_2 = p_2q_2$ and e_2.
For Bob to communicate with Alice, he takes his message M encrypts by

$$M_1^e mod n_1.$$

But anyone could have sent this message to Alice. How can Bob ensure that Alice knows that he sent the message.
Instead, Bob should send the following:

$$(M_1^e mod n_1)_2^d mod n_2.$$

To decrypt the message, Alice would first have to encrypt it using Bob's public encrypting exponent e_2 then decrypt using her own decrypting exponent d_1. Since only Bob knows his decrypting exponent, the message will wind up being incomprehensible unless it was really Bob who sent the message.

Exercises

1. An individual publishes an RSA modulus of $m = 350123$ and an encryption exponent $e = 37$. Find his decrypting exponent, given that one of the factors of m is 347.

2. Encrypt each letter of the word `BANG` individually using the RSA system with $m = 143$ and $e = 7$. In translating letters into numbers, send `A` to 10, `B` to 11, ..., `Z` to 35.

3. Using the same system described in the previous problem, find the decrypting exponent d and decode the message 132 (a single letter).

4. Factor $m = 773,771$ into the product of two primes given that $\phi(m) = 771,552$.