# Lecture 3: Public Key Cryptography

Note Title 9/15/2010

In traditional crytography, messages are coded with an encrytion key (enciphering key). The recipient receives the coded message and decode it with the decryption key (deciphering key). Once you know the encrytion key you will know the decryption key.

As an example let us consider the Hill 2-cipher of the message MATH, which corresponds to the numbers 12 0 19 7. Assume the encryption matrix is

$$\mathcal{E} = \begin{bmatrix} 5 & 10 \\ 1 & 3 \end{bmatrix}.$$

Now $\quad MA \longrightarrow \begin{bmatrix} 12 \\ 0 \end{bmatrix}, \quad TH \longrightarrow \begin{bmatrix} 19 \\ 7 \end{bmatrix}.$ The ciphered message is now given by

$$\mathcal{E}\begin{bmatrix} 12 \\ 0 \end{bmatrix} \pmod{26} = \begin{bmatrix} 60 \\ 12 \end{bmatrix} \pmod{26} = \begin{bmatrix} 6 \\ 12 \end{bmatrix} \longrightarrow GM$$

and

$$\mathcal{E}\begin{bmatrix} 19 \\ 7 \end{bmatrix} \pmod{26} = \begin{bmatrix} 165 \\ 40 \end{bmatrix} \pmod{26} = \begin{bmatrix} 9 \\ 14 \end{bmatrix} \longrightarrow JO$$

Thus the ciphered text is GMJO (or 6 12 9 14).

Assume now you are the secret agent who has obtained the encrytion key $\mathcal{E}$ and the ciphered text 6 12 9 14. You can invert the matrix $\mathcal{E}$ to obtain the deciphering key $\mathcal{F}$. In this case the deciphering key $\mathcal{F}$ is a $2 \times 2$ matrix such that

$$\mathcal{F}\mathcal{E} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}.$$

To see how does it work, we're looking for messages $\vec{x}, \vec{y}$ such that

$$\mathcal{E}\vec{x} = \begin{bmatrix} 6 \\ 12 \end{bmatrix} \pmod{26}, \qquad \mathcal{E}\vec{y} = \begin{bmatrix} 9 \\ 14 \end{bmatrix} \pmod{26}$$

Now

$$\vec{x} \equiv \mathcal{F}\mathcal{E}\vec{x} \equiv \mathcal{F}\begin{bmatrix} 6 \\ 12 \end{bmatrix} \pmod{26},$$

$$\vec{y} \equiv \mathcal{F}\mathcal{E}\vec{y} \equiv \mathcal{F}\begin{bmatrix} 9 \\ 14 \end{bmatrix} \pmod{26},$$

which allows to decipher $\vec{x} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \to$ MA, $y = \begin{bmatrix} 19 \\ 7 \end{bmatrix} \to$ TH.

Note that in $2 \times 2$ case $\mathcal{F}$ is quite easily obtained. We've

$$\begin{bmatrix} 3 & -10 \\ -1 & 5 \end{bmatrix}\mathcal{E} = \begin{bmatrix} 3 & -10 \\ -1 & 5 \end{bmatrix}\begin{bmatrix} 5 & 10 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

and $21 \cdot 5 \equiv 1 \pmod{26}$, i.e. $5^{-1} \pmod{26} = 21$.

So
$$\mathcal{F} \equiv 21 \cdot \begin{bmatrix} 3 & -10 \\ -1 & 5 \end{bmatrix} \equiv \begin{bmatrix} 11 & 24 \\ 5 & 1 \end{bmatrix} \pmod{26}.$$

We've found the decrytion key $\mathcal{F}$!

In public key cryptography, the encryption key is chosen so that it is not practically invertible. Thus even if one knows the encryption, she cannot find the decryption key in a practical time frame and break the cipher. We shall present one such scheme: The RSA encryption.

Before doing so we'll need some basic knowledge of modular arithmetic. We've already introduced $\mathbb{Z}_m$, in particular $m=26$. In this lecture we will go into more details. Special attentions will be paid to $\mathbb{Z}_p$ where $p$ is a prime number.

We've already gone over addition, subtraction and multiplication in $\mathbb{Z}_m$. To complete the arithmetic operations on $\mathbb{Z}_m$ we must also consider divisions. For example, on $\mathbb{Z}_{26}$ what is $10/7$? What does it mean? Does it exist, and if so is it unique? These are some of the questions we need to answer. Clearly there is a natural way to consider division on $\mathbb{Z}_m$ such as $10/7$ on $\mathbb{Z}_{26}$. Call $x = 10/7$ on $\mathbb{Z}_{26}$. Then

$$7x \equiv 10 \pmod{26}$$

So the real questions are :

① Is there an $x$ in $\mathbb{Z}_{26}$ such that $7x \equiv 10 \pmod{26}$ ?

② If yes, is it unique ?

As it turns out, both answers are affirmative. You can check $x \equiv 20 \pmod{26}$ has $7x \equiv 140 \equiv 10 \pmod{26}$, and it is the only one. So $10/7 = 20$ in $\mathbb{Z}_{26}$.

Note that $10/7 = 10 \cdot \frac{1}{7}$ in $\mathbb{Z}_{26}$. So if we can have $1/7$ then we can have any $a/7$ in $\mathbb{Z}_{26}$. It is easy to check $1/7 = 15$ in $\mathbb{Z}_{26}$. We shall denote

$$7^{-1} = 15 \quad \text{in } \mathbb{Z}_{26} \, , \quad \text{or} \quad 7^{-1} \equiv 15 \pmod{26}.$$

Not every element in $\mathbb{Z}_m$ has an inverse. For example, $2$ in $\mathbb{Z}_{26}$ has no inverse. We've

**Theorem 1** Let $a \in \mathbb{Z}_m$. Then $a^{-1}$ exists in $\mathbb{Z}_m$ if $\gcd(a, m) = 1$, i.e. $a, m$ are coprime.

Proof Multiply all elements in $\mathbb{Z}_m$ by $a$ we get

$$0 \, , \, a \, , \, 2a \, , \, \cdots , \, (m-1)\, a \pmod{m}.$$

We claim that they are all distinct in $\mathbb{Z}_m$. Assume the contrary is true, then we'll have

$$ka \equiv la \pmod{m}$$

for some $0 \leq k, l < m$, $k \neq l$. Thus

$$(k-l)a \equiv 0 \pmod{m},$$

i.e.

$$m \mid (k-l)a.$$

But $m, a$ are coprime, so we must have $m \mid k-l$. Thus, $k \equiv l \pmod{m}$. This is not possible, a contradiction.

Therefore we conclude that $0, a, 2a, \cdots, (m-1)a \pmod{m}$ are all distinct. Observe that we've $m$ elements here, which is the same as the number of elements in $\mathbb{Z}_m$. It means that they simply represent a permutation of elements in $\mathbb{Z}_m$. In particular, one and only one of them is $1 \pmod{m}$, say $ka \equiv 1 \pmod{m}$. It follows that $a^{-1} \pmod{m}$ is $k$, and it's unique.

☒

It should be mentioned that the converse is also true, i.e. if $a$ is not coprime to $m$ then $a^{-1}$ does not exist. Can you prove it?

**Corollary** Let $p$ be a prime. Then $a^{-1}$ exists for any nonzero $a$ in $\mathbb{Z}_p$.

Proof Any $a \neq 0$ in $\mathbb{Z}_p$ is coprime with $p$. ☒

An important theorem for our discussion is

**Fermat's Little Theorem** Let $p$ be a prime. Then for any $a$ we've

$$a^p \equiv a \pmod{p}.$$

If $a$ is not divisible by $p$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof If $p | a$ then $p | a^p$, so $p | a^p - a$, and hence $a^p \equiv a \pmod{p}$.

If $p \nmid a$ then $p$ is coprime to $a$. By our previous discussions, $a, 2a, \cdots, (p-1)a \pmod{p}$ is a permutation of $1, 2, \cdots, p-1$ in $\mathbb{Z}_p$. Thus

$$a \cdot (2a) \cdot (3a) \cdot \cdots (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}$$

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

But $(p-1)!$ is coprime to $p$, and let $x = (p-1)!^{-1}$ in $\mathbb{Z}_p$. We've

$$x\,(p-1)!\, a^{p-1} \equiv x\,(p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

☒

An important Corollary of this theorem is

**Corollary** Let $p, q$ be two different primes. Assume $a$ is coprime to both $p, q$. Then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Proof Let $b = a^{q-1}$. Then $p \nmid b$. So

$$b^{p-1} = a^{(p-1)(q-1)} \equiv 1 \pmod{p}.$$

Similarly, let $c = a^{p-1}$. Then $q \nmid c$. So

$$c^{q-1} = a^{(p-1)(q-1)} \equiv 1 \pmod{q}.$$

All these mean

$$p, q \mid a^{(p-1)(q-1)} - 1.$$

Hence

$$pq \mid a^{(p-1)(q-1)} - 1.$$

☒

## RSA Cryptosystem

RSA is named after Rivest, Shamir and Adleman, 3 computer scientists and mathematicians at MIT. The system was in fact first devised by the British mathematician Clifford Cocks in 1973. But with limited computing power at the time it was nothing more than a curiosity. The MIT team came up with it independently.

In the RSA system, the encryption key is a pair of integers $(N, e)$, where $N = pq$ is the product of two primes, $p \neq q$, and $e$ is large and coprime to $(p-1)\cdot(q-1)$.

**How (N, e) works** Say we've a message $m$ (by now you are familar with coding letters with numbers). We'll need $N$ to be fairly large so $m < N$.

Encryption: $m \longmapsto m^e \pmod N$

The computation for $m^e \pmod N$ can be very fast.

**Example 1** Let $N = 3 \times 11 = 33$ and $e = 7$. Clearly $e$ is coprime to $(3-1)(11-1) = 20$. Say the message is $m = 2$ (the letter C). Then it is ciphered into

$$2 \longmapsto 2^7 \pmod{33} \equiv \underline{\underline{29}} \pmod{33}.$$

**Example 2** Let $N = 281 \times 167 = 46927$, $e = 39423$.

Say messages in letters are converted into numbers using 3-letter combinations. In this case, YES is

$$m = 24\cdot 26^2 + 4\cdot 26 + 18 = 16346$$

To encipher $m$, we do

$$m^e \pmod N \equiv 16346^{39423} \pmod{46927}$$

$$\equiv 21166 \pmod N$$

$$1\cdot 26^3 + 5\cdot 26^2 + 8\cdot 26 + 2 \rightarrow \text{BFIC}.$$

## Deciphering key

The enciphering key $(N, e)$, where $N = pq$, encrypt a message $m$ into

$$C \equiv m^e \pmod N.$$

To decipher the encrypted message $C$, we use the deciphering key $(N, d)$. Here $d$ is given by

$$d = e^{-1} \pmod{(p-1)(q-1)}.$$

Call $K = (p-1)(q-1)$. As long as $p, q \nmid m$ we'll have

$$m^K \equiv 1 \pmod N$$

by the corollary to Fermat's Little Theorem. Now, from the encrypted message $C$ we can decipher it using $(N, d)$ as follows: Not that $de \equiv 1 \pmod K$. So

$$de = 1 + nK \quad \text{for some } n.$$

Thus

$$C^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+nk}$$

$$\equiv m \cdot (m^k)^n \equiv m \cdot 1^n$$

$$\equiv m \pmod N$$

We've therefore recovered $m$ using $(N, d)$.

**Example** We go back to the first example where $N = 3 \cdot 11 = 33$ and $e = 7$. $K = 2 \times 10 = 20$. Now $d \equiv e^{-1} \equiv 7^{-1} \pmod{20} = 3$. So the deciphering key is $(33, 3)$. For the encrypted message $C = 29$, the deciphered message is

$$m \equiv C^3 \equiv 29^3 \equiv 2 \pmod{33},$$

which recovers the original message.

**Example** We go back to the second example, where $(N, e) = (46927, 39423)$, with $N = 281 \times 167$. $K = 280 \times 166 = 46480$. One can check

$$d \equiv e^{-1} \pmod K = 26767.$$

So the deciphering key is $(46927, 26767)$. Using this we can recover the original message $m$ from the Ciphered message $C = 21166$.

$$M \equiv C^{d} \equiv 21166^{26767} \pmod{46927}$$

$$\equiv 16346 \pmod{46927}$$

Check it out using a calculator.

## Why is RSA a Public Key Cryptosystem?

To find the deciphering key $(N, d)$ from the enciphering key $(N, e)$, we compute

$$d \equiv e^{-1} \pmod{K}$$

where $N = pq$, $K = (p-1)(q-1)$. This in itself is quite easy to do if we know $K$. But here is the beauty: To know $K$ we need to know $p, q$, i.e. we need to know the factorization of $N$. If $p, q$ are both very large, say each is over 150 digits long, this is practically impossible to do! So in practice it is impossible to find $(N, d)$.

## Other Questions

1. Where do we find very large primes $p, q$?

As it turns out, there is a very efficient way to find large primes. Please google primality test to know more about it.

**2. With very large numbers $m, N, e$, is it very expensive to compute $m^e \pmod N$?**

The answer is NO. It can be done very efficiently. This can be seen from an example:

e.g. Compute $127^{1024} \pmod{1000}$.

$$127^{1024} = (127^2)^{512} = (16129)^{512} \equiv 129^{512} \pmod{1000}$$

$$= (129^2)^{256} = 16641^{256} \equiv 641^{256} \pmod{1000}$$

$$= (410881)^{128} \equiv 881^{128} \pmod{1000}$$

$$= (881^2)^{64} = 776161^{64} \equiv 161^{64} \pmod{1000}$$

$$= (161^2)^{32} = 25921^{32} \equiv (-79)^{32} \equiv 79^{32}$$

$$= 6241^{16} \equiv 241^{16} \equiv 58081^{8} \equiv 81^{8}$$

$$\equiv 6561^{4} \equiv 561^{4} \equiv 314721^{2} \equiv 721^{2}$$

$$\equiv 519841 \equiv 841 \pmod{1000}$$