Abstract. In this lecture we introduce necessary mathematical background for studying the RSA public key cryptosystem. Readings from Chapter 5 of D. Stinson.

1 Public Key Cryptosystems

The idea of public keys is that Alice uses a key $K^{-1}_A$ to encrypt and Bob uses key $K_A$ to decrypt, with $K_A \neq K^{-1}_A$, i.e. encryption and decryption use different keys (asymmetric encryption/decryption).

1.1 Euler’s $\phi$-function

$\phi(n)$ is defined as the number of integers less than $n$ and relatively prime to $n$.

Examples:
1. If $p$ is a prime then, $\phi(p) = p - 1$, since $\{1, 2, ..., p - 1\}$ are relatively prime to $p$.
2. $\phi(2) = 1, \{1\}$.
3. $\phi(3) = 2, \{1, 2\}$.
4. $\phi(4) = 2, \{1, 3\}$.
5. $\phi(6) = 2, \{1, 5\}$.
6. $\phi(p^2) = p^2 - \frac{p^2}{p} = p(p - 1)$, every other $p^{th}$ element is divided by $p$.
7. Let $p, q$ be primes, $p \neq q$. Then, $\phi(pq) = pq - (p + q - 1)$ (remove $p + q - 1$ elements from pq elements). Further simplifying we get, $\phi(pq) = (p - 1)(q - 1) = \phi(p)\phi(q)$. (Think of $\phi(pq) = \prod (p^i - p^0) \times (q^i - q^0)$.)

1.2 The Euclidean Algorithms

Let $\mathbb{Z}_n^*$ denote the set of residues relatively prime to $n$. Any element in $\mathbb{Z}_n^*$ will have a multiplicative inverse also in $\mathbb{Z}_n^*$. Problem is how do we find such inverse (remember we used this inverse to decrypt affine ciphers).

The Euclidean GCD algorithm First, we present the Euclidean algorithm for finding the $gcd$ of two numbers $(a, b)$.

Let $a = bq + r$, then find a number $u$ which divides both $a$ and $b$ (so that $a = su$ and $b = tu$), then $u$ also divides $r$ since

$$r = a - bq = su - qt u = (s - qt)u. \quad (1)$$

Similarly, find a number $v$ which divides $b$ and $r$ (so that $b = s'v$ and $r = t'v$), then $v$ divides $a$ since

$$a = bq + r = qs'v + t'v = (qs' + t')v. \quad (2)$$
Therefore, every common divisor of $a$ and $b$ is a common divisor of $b$ and $r$, and the procedure can be iterated as follows:

\[
a = r_0 = q_1 r_1 + r_2, \quad 0 < r_2 < r_1, \quad q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor
\]

\[
b = r_1 = q_2 r_2 + r_3, \quad 0 < r_3 < r_2, \quad q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor
\]

\[
\vdots
\]

\[
r_{m-2} = q_{m-1} r_{m-1} + r_m, \quad 0 < r_m < r_{m-1}, \quad q_{m-1} = \left\lfloor \frac{r_{m-2}}{r_{m-1}} \right\rfloor
\]

\[
r_{m-1} = q_m r_m.
\]

(3)

It follows that

\[
\gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{m-1}, r_m) = r_m,
\]

(4)

and hence, $\gcd(a, b) = \gcd(r_0, r_1) = r_m$.

**Example** $(a, b) = (42, 30)$.

\[
42 = 1 \times 30 + 12
\]

\[
30 = 2 \times 12 + 6
\]

\[
12 = 2 \times 6
\]

(5)

and the $\gcd(42, 30) = 6$

**Example** $(a, b) = (144, 55)$.

\[
144 = 2 \times 55 + 34
\]

\[
55 = 1 \times 34 + 21
\]

\[
34 = 1 \times 21 + 13
\]

\[
21 = 1 \times 13 + 8
\]

\[
13 = 1 \times 8 + 5
\]

\[
8 = 1 \times 5 + 3
\]

\[
5 = 1 \times 3 + 2
\]

\[
3 = 1 \times 2 + 1
\]

\[
2 = 2 \times 1
\]

and the $\gcd(144, 55) = 1$ (the two numbers are relatively prime).

Define the following two sequences of numbers

\[
t_0, t_1, t_2 \ldots t_m, \quad s_0, s_1, \ldots, s_m
\]

(6)

with $t_0 = 0$, $t_1 = 1$, $t_j = t_{j-2} - q_{j-1} t_{j-1}$ and $s_0 = 1$, $s_1 = 0$, $s_j = s_{j-2} - q_{j-1} s_{j-1}$. Then
Theorem 1. For \( 0 \leq j \leq m \), \( r_j = s_j a + t_j b \).

Proof. Can be proved via induction

Extended Euclidean Algorithm Let \((a, b)\) be two integers. We compute integers \(r, s, t\) such that \( r = \gcd(a, b) \) and \( sa + tb = r \)

Corollary 1. Let \( \gcd(r_0, r_1) = 1 \) (condition for the existence of \( r_1^{-1} \)). Then \( r_1^{-1} \mod r_0 = t_m \mod r_0 \).

Proof. From previous theorem \( r_m = s_m r_0 + t_m r_1 \), but \( r_m = \gcd(a, b) = 1 \). Hence,

\[
\begin{align*}
    s_m r_0 + t_m r_1 &= 1 \\
t_m r_1 &= 1 \pmod{r_0}
\end{align*}
\]

Example: We want to calculate \( 28^{-1} \mod 75 \).

\[
\begin{array}{c|c|c|c|c}
    i & r_i & q_i & s_i & t_i \\
    
    0 & 75 & 1 & 0 \\
    1 & 28 & 2 & 0 & 1 \\
    2 & 19 & 1 & 1 & -2 \\
    3 & 9 & 2 & -1 & 2 \\
    4 & 1 & 9 & 3 & -8 \\
\end{array}
\]

Therefore \( 3 \times 75 - 8 \times 28 = 1 \). Based on Corollary 1, \( 28^{-1} \mod 75 = -8 \mod 75 = 67 \).

1.3 Chinese Remainder Theorem

Let \( m_1, m_2, ..., m_r \) be integers such that \( \gcd(m_i, m_j) = 1 \), \( i \neq j \) (relatively prime). Then the set of congruences \( X \equiv a_i \mod m_i \), \( i = 1, 2, ..., r \), has a unique solution modulo \( M \), where \( M = m_1 m_2 ... m_r = \prod_{i=1}^{r} m_i \).

Proof: Let \( M_i = \frac{M}{m_i} \). Note \( \gcd(M_i, m_i) = 1 \).

Let \( y_i = M_i^{-1} \mod m_i \Rightarrow M_i y_i = 1 \mod m_i \) (The inverse exists because \( \gcd(M_i, m_i) = 1 \), and can be found using the Extended Euclidean Algorithm).

Let \( \rho(a_1, a_2, ..., a_r) = \sum_{i=1}^{r} a_i M_i y_i \mod M \), be the solution.

Denote \( X = \rho(a_1, a_2, ..., a_r) \) and let \( 1 \leq j \leq r \). Consider a term of \( \rho \) reduced modulo \( m_j \). If \( i = j \)

\[ a_i M_i y_i = a_j \mod m_i \], because \( M_i y_i \equiv 1 \mod m_i \).

If \( i \neq j \)

then \( a_i M_i y_i \equiv 0 \mod m_j \) since \( m_j | M_i \).

Hence, \( X = \sum_{i=1}^{r} a_i M_i y_i \mod m_j \equiv a_j \mod m_j \).
This is true for all \( j \) and hence \( X \) is a solution to the system of congruences. This solution can also be shown to be unique modulo \( M \) since the cardinalities of the domain and the range are equal.

**Example:**

Solve the system of congruences

\[
X \equiv 5 \pmod{7} \\
X \equiv 3 \pmod{11} \\
X \equiv 10 \pmod{13}
\]

- **Step 1:** \( r = 3, m_1 = 7, m_2 = 11, m_3 = 13, a_1 = 5, a_2 = 3, a_3 = 10, M = 7 \times 11 \times 13 = 1001 \).
- **Step 2:** \( M_1 = 143, M_2 = 91, M_3 = 77 \).
- **Step 3:** Use Extended Euclidean Algorithm and find \( y_1 = 5, y_2 = 4, y_3 = 12 \).
- **Step 4:** Compute

\[
X = (5 \times 143 \times 5) + (3 \times 91 \times 4) + (10 \times 77 \times 12) \mod 1001 = 894
\]

- **Step 5:** Verify \( 894 \equiv 5 \pmod{7} \), \( 894 \equiv 3 \pmod{11} \), \( 894 \equiv 10 \pmod{13} \).

Note that \( X \pmod{M} = a_1 \pmod{m_1} = \ldots a_r \pmod{m_r} \) (we will use this fact in the RSA cryptosystem).

### 1.4 Euler’s Theorem

**Given** \( gcd(a, n) = 1 \), then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

Let \( Z_n^* = \{x_1, x_2, ..., x_{\phi(n)}\} \) be such that \( gcd(x_i, n) = 1 \). Let \( S = \{ax_1, ax_2, ..., ax_{\phi(n)}\} \) be elements of \( ax_i \mod n \).

**Claims:**

1. \( ax_i \neq ax_j \) if \( x_i \neq x_j \).  
2. \( ax_i \neq 0 \) if \( x_i \neq 0 \). That is \( S \) is a permutation of \( Z_n^* \).

**Proof of the claims and theorem:**

1. **(By contradiction:)** Let \( x_i \neq x_j \), but \( ax_i = ax_j \mod n \).

   Note,

   \[
   0 \leq x_i \leq n - 1, \\
   0 \leq x_j \leq n - 1 \\
   \Rightarrow -(n - 1) \leq x_i - x_j \leq (n - 1), \\
   |x_i - x_j| \leq n - 1.
   \]

   Now, if \( ax_i = ax_j \mod n \Rightarrow n|a(x_i - x_j) \).

   1 Note that \( gcd(a, n) = 1 \Rightarrow n \) does not divide \( a \). Hence \( n|(x_i - x_j) \Rightarrow n \) divides \( |x_i - x_j| \). But we have \( |x_i - x_j| \leq n - 1 < n \).

   So \( n \) divides \( x_i - x_j \), but \( x_i - x_j < n \Rightarrow x_i - x_j = 0 \), i.e. \( x_i = x_j \). This contradicts with initial assumption that \( x_i \neq x_j \).

   Hence if \( x_i \neq x_j \Rightarrow ax_i \neq ax_j \).

1 Recall that \( a|b \) indicates \( a \) divides \( b \)
(2) Assume that for some element $x$, $ax = 0 \mod n$. That means that either $n|a$ or $n|x$. But $gcd(a, n) = 1$ and $gcd(x, n) = 1$, hence $ax \neq 0$.

Hence this implies that no element of $S$ is $0$, and $S$ is a permutation of $Z_n^*$.

From the above two claims, we can now prove Euler’s theorem as follows.

Multiply all elements of $Z_n^*$ to get $x_1 x_2 \ldots x_{\phi(n)} = \prod_{i=1}^{\phi(n)} x_i$.

Multiply all elements of $S$ to get $a x_1 a x_2 \ldots a x_{\phi(n)} = a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i$.

$\Rightarrow \prod_{i=1}^{\phi(n)} x_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i \mod n$ (because of the permutation property the two products are congruent modulo $n$).

$gcd(x, n) = 1 \Rightarrow a^{\phi(n)} = 1 \mod n$. This is Euler’s Theorem.

Example: $a = 2, n = 11, \phi(n) = 10$. Then, $a^{\phi(n)} \equiv 2^{10} \equiv 1024 \equiv 93 \times 11 + 1 \equiv 1 \mod 11$.

Note that if $n = p$, a prime, then $\phi(n) = p - 1 \Rightarrow a^{p-1} = 1 \mod p$. This is Fermat’s Little Theorem.

2 RSA Public Key Cryptosystem

2.1 Basic Idea of RSA

Alice chooses two distinct primes $p, q$, and sets $n = pq$. Now, $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$. Alice then picks $a, b$ to set $ab \equiv 1 \mod \phi(n)$, i.e. $ab = 1 + \lambda \phi(n)$. Then the encryption key (public key) of Alice, $K_A = (b, n)$, and decryption key (private key), $K_{A^{-1}} = (a, n)$. The encryption and decryption algorithms are:

$$c = E_{K_A}(m) = m^b \mod n,$$

$$D_{K_A}(c) = x = c^a \mod n,$$

$$= (m^b)^a \mod n,$$

$$= m^{ab} \mod n.$$  

Now since $ab \equiv 1 \mod \phi(n)$, $ab \equiv 1 (\mod \phi(n))$ and $ab \equiv 1 (\mod \phi(q))$.

Let $ab = k\phi(p) + 1$. If $m$ is not a multiple of $p$, $m \in Z_n^*$, that is $m, p$ are relatively prime, since $m$ is prime. In that case we can apply Euler’s theorem (Fermat’s little theorem) and obtain:

$$m^{ab} \mod p = m^{k\phi(p)+1} \mod p = (m^{\phi(p)})^k m \mod p \equiv 1^k m \mod p \equiv m \mod p. \quad (9)$$

If $m$ is a multiple of $p$ it follows that $m^{ab} \mod p \equiv 0 \mod p \equiv m \mod p$. Hence in any case $m^{ab} \equiv m \mod p$.

Similarly we can obtain that $m^{ab} \equiv m \mod q$. Now for the system of congruences we can apply the Chinese Remainder Theorem and obtain that $m^{ab} \mod n = m \mod n$. 


2.2 Implementation of the RSA Algorithm

1. Choose two large primes \( p, q \) with \( p \neq q \) and let \( n = pq \).
2. Randomly choose \( b \) with \( 1 < b < \phi(n) \) such that \( \gcd(b, \phi(n)) = 1 \).
3. Compute \( a = b^{-1} \mod \phi(n) \).
4. The public key is \((b, n)\) and the private key is \((n, a)\).
5. Encryption of a message using the public key is \( c = E_{(b, n)}(m) = m^b \mod n \).
6. Decryption of the ciphertext is \( D_{(a, n)}(c) = c^a \mod n \).

Note: As we will see later in digital signatures, Alice can use \((a, n)\) as the signing key, while Bob’s verification key is \((b, n)\).

2.3 How many primes are there?

Because we need primes for RSA, an interesting question to ask is “how many primes are there?”. A proof was given by Euler. It is as follows. Assume there are \( k \) distinct primes only, \( p_1, p_2, \ldots, p_k \). Define the integer \( l = \prod_{j=1}^{k} p_j + 1 \). Note that each \( p_i, i = 1, 2, \ldots, k \) divides \( \prod_{j=1}^{k} p_j \). We denote this as \( p_i | \prod_{j=1}^{k} p_j, i = 1, 2, \ldots, k \).

Now if \( l \) is not a prime, then it is divisible by \( p_i, i = 1, 2, \ldots, k \). i.e. \( p_i | l = p_i | (\prod_{j=1}^{k} p_j + 1) \).

Because \( p_i | \prod_{j=1}^{k} p_j \), then \( p_i | 1 \), and this implies that \( p_i = 1, i = 1, 2, \ldots, k \). But this contradicts with the fact that the \( p_i \)’s are distinct primes. Hence \( p_i \) does not divide \( l \), which implies that \( l \) is not divisible by any of the primes we know so far. Therefore, there must be another prime that divides \( l \). We have found a new prime! This continues....

2.4 Examples for RSA

(1) Eve claims that if she knows \( n \) and \( \phi(n) \), she can factor \( n \). How?

\[
\begin{align*}
n &= pq, \\
\phi(n) &= (p-1)(q-1) = pq - (p + q) + 1, \\
\Rightarrow n - \phi(n) &= p + q - 1, \\
\Rightarrow p + q &= n - \phi(n) + 1.
\end{align*}
\]

Since \( pq = n \), we can write, \((X - p)(X - q) = X^2 - (p + q)X + pq = X^2 - (n - \phi(n) + 1)X + n\).

The solution is \( p, q = \frac{n - \phi(n) + 1 \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2} \).

Supposing \( n = 221 \) then \( \phi(n) = 192 \) and, \( p, q = \frac{(221 - 192 + 1) \pm \sqrt{(221 - 192 + 1)^2 - 4 \times 221}}{2} = 13, 17. \)

(2) If Eve knows \( a, b \), she can possibly factor \( n \). We will see this later.

(3) Given \( n = 11413 = 101 \times 113, b = 7467. \) Find \( a \) such that \( ab = 1 \mod \phi(n) \).

\( \phi(n) = \phi(101 \times 113) = \phi(101)\phi(113) = 100 \times 112. \) Then,
\(ab \equiv 1 \mod (100 \times 112),\)
\(ab = 1 + \lambda(100 \times 112),\)
\(= 1 + \lambda(4 \times 25 \times 16 \times 7),\)
\(ab = 1 + \lambda(7 \times 25 \times 64).\)

\[\Rightarrow ab \equiv 1 \mod 7,\]
\(ab \equiv 1 \mod 25,\)
\(ab \equiv 1 \mod 64.\)

The last three congruences are a result of the application of the Chinese Remainder Theorem to \(ab \equiv 1 \mod (7 \times 25 \times 64).\)

Now, \(a = 7467 \equiv 5 \mod 7.\) Then, \(7467b \equiv (5)b \equiv 1 \mod 7.\)

We get, \(5d = 1 + \lambda(7) = 1 + \lambda(5 + 2),\) i.e. \(5d = (1 + 2\lambda) + 5\lambda.\)

We now need to choose \(\lambda\) such that \((1 + 2\lambda)\) is divisible by 5.

Setting \(\lambda = 2,\) we get \(1 + 2\lambda = 5.\) And \(5b = (1 + 2\lambda) + 5\lambda = 15 \Rightarrow b = 3.\)

Hence the keys are \((a, b) = (7467, 3).\)

(4) Assume that \(p\) is a prime, and that \(m = x,\) and \(c = x^h \mod p.\) How to find \(a\) such that \(c^a \equiv x \mod p?\)

Note that \(c^a = (x^h)^d = x^{ab} \mod p.\) Using Fermat’s Little Theorem/Euler’s theorem,
\(\gcd(x, p) = 1 \Rightarrow x^{p-1} \equiv 1 \mod p.\)
\(\Rightarrow x^{ab} \equiv x \equiv x^{\lambda(p-1)} x \mod p.\)
\(\Rightarrow ab = 1 + \lambda(p - 1),\)
\(\Rightarrow ab \equiv 1 \mod (p - 1).\)