Week 6

Topics: More on RSA
Primality Testing
ElGamal Cryptosystem
Elliptic curve over Reals
Elliptic curve modulo Prime

Computational Aspects of RSA:

The complexity of computation required boils down to two aspects:

1. The actual encryption / decryption process

2. The key generation process.

1. Encryption and Decryption:

- Both involve raising a large integer to a large integer power modulo n.

- Suppose we wish to find the value a^m where a, m positive integers.

- If we express m as a binary number $b_k b_{k-1} \cdots b_0$ then,

$$m = \sum_{i=0}^{k} b_i 2^i = \sum_{b_i \neq 0} 2^i$$

- Therefore,

$$a^m = a^{\sum_{b_i \neq 0} 2^i} = \prod_{b_i \neq 0} a^{2^i}$$

$$\Rightarrow a^m \bmod n = \left[\prod_{b_i \neq 0} a^{2^i}\right] \bmod n$$

$$= \left[\prod_{b_i \neq 0} (a^{2^i} \bmod n)\right] \bmod n$$

- This can be doem using square and multiply algorithm:

Input: a, $m = (b_k b_{k-1} \cdots b_0)_{10}$

1. $z = 1$
2. for $i = k$ down to 0 do
3. $\quad z = z^2 \bmod n$
4. $\quad$ if $b_i = 1$ then $z = z \times a \bmod n$
5. return z

- **Example:** Let $n = 11413$, $m = 3533$, $a = 9726$. Compute $9726^{3533} \pmod{11413}$

Use square and multiply algorithm:

i	b_i	z
11	1	$1^2 \times 9726 = 9726$
10	1	$9726^2 \times 9726 = 2659$
9	0	$2659^2 = 5634$
8	1	$5634^2 \times 9726 = 9167$
7	1	$9167^2 \times 9726 = 4958$
6	1	$4958^2 \times 9726 = 7783$
5	0	$7783^2 = 6298$
4	0	$6298^2 = 4629$
3	1	$4629^2 \times 9726 = 10185$
2	1	$10185^2 \times 9726 = 105$
1	0	$105^2 = 11025$
0	1	$11025^2 \times 9726 = 5761$

All multiplications are modulo 11413.

- Therefore $9726^{3533} \bmod 11413 = 5761$

2. Key Generation :

- We use $n = pq$ where p, q are sufficiently large primes.
- At present there are no useful techniques that yield arbitrarily large primes.
- The procedure is to pick a random integer (odd) of desired magnitude and test whether it is prime. If not repeat.
- Testing an integer prime is a probabilistic algorithm.
- One of the more efficient algorithms is Miller - Rabin Scheme.
- - Pick an odd integer n at random (use PRG (pseudorandom number generator))
  - Pick a $a < n$ at random
  - check a is prime. If fail then repeat from picking $a < n$.
  - Run sufficient number of times for n. If no $a < n$ found to be prime, change n.

• Primality Testing :

- **Problem :** Given an odd integer p.
  Need to verify whether p is prime, i.e, p has only two divisors 1 and p itself.

Solutions :

1. **Naive Algorithm :**

- For every integer n there is a factor of n which is less than or equal to $\sqrt{n}$.

- Let $K \in \{1, 2, \ldots, \sqrt{p}\}$.

If K is a factor of p then p is not a prime if $K > 1$.

Therefor we need to check all the integers from 2 to $\sqrt{p}$ whether it divides p or not, to ensure the primality of p.

But if p is large then this solution is not suitable to the above problem.

2. Sieve of Eratosthenes :

- It is used to locate all primes upto a specified positive integer n.
- Start by writing the integers 2, 3, 4, ..., n in a list.

  Then enters into a loop, each iteration of which discovers a new prime and marks all multiples of that prime (other than the prime itself) as composite.
- The first unmarked integer is 2, which is marked as prime. All even integers in the list larger than 2 are marked as composite.
- In the second pass, the first unmarked integer 3 is marked as prime. All multiples of 3 are marked as composite.
- This process repeated untill the first unmarked entry exceeds $\sqrt{n}$.
- All the unmarked integers are prime.

Example: Let $n = 20$. $5 > \sqrt{20}$

	[2]	3	4	5	6	7	8	9	10	} pass 1
11	12	13	14	15	16	17	18	19	20	
	[2]	[3]	4	5	6	7	8	9	10	} pass 2
11	12	13	14	15	16	17	18	19	20	
	[2]	[3]	4	[5]	6	7	8	9	10	} pass 3
11	12	13	14	15	16	17	18	19	20	
	[2]	[3]	4	[5]	6	[7]	8	9	10	} pass 4
11	12	13	14	15	16	17	18	19	20	

Note we do not need pass 3 and pass 4 as we already get all primes in pass 2. It is because first unmarked entry in pass 2 is 5 which is larger than $\sqrt{20}$.

Hence all primes are 2, 3, 5, 7, 11, 13, 17, 19.

3. Fermat Test :

- By Fermat's little theorem, $a^{n-1} \equiv 1 \pmod{n}$ for every $a \in \mathbb{Z}_n^*$ if n is prime.

  But converse is not true.

  Example → $n = 17343$, $a = 163$

  check $a^{n-1} \equiv 1 \pmod{n}$ but n is not prime.

- Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$

We call n a pseudo prime (or a Fermat pseudo prime) to the base a if

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

Fermat Primality Testing → Input : integer p.

1. choose $a < p$
2. compute $\gcd(a,p)$
3. If $\gcd(a,p) > 1$
4. then return "p is composite"
5. If $\gcd(a,p) = 1$
6. $y \leftarrow a^{p-1} \pmod{p}$
7. If $(y \not\equiv 1 \pmod{p})$
8. then return "p is composite".
9. else return "p is prime".

- Fermat Primality Testing is a probabilistic algorithm. If it returns p is composite then p is definitely composite. But if it returns p is prime then there is a probability that p may be composite.

- **Example:** Let $p = 49$, $a = 19$

  Then $\gcd(p, a) = 1$.

  $a^{p-1} = 19^{48} \equiv 1 \pmod{49}$

  $\Rightarrow$ 49 is a ~~Fair~~ Fermat pseudoprime base 19.

  Let $a = 31$. Then $a^{p-1} = 31^{48} \equiv 1 \pmod{49}$

  $\Rightarrow$ 49 is a Fermat pseudoprime base 31

  Let $a = 5$. Then $a^{p-1} \equiv 5^{48} \not\equiv 1 \pmod{49}$

  $\Rightarrow$ 49 is composite.

4. Miller - Rabin Primality testing :

- Let p be a prime.

Then, $p - 1 = 2^k m$ where m is odd.

$$a^{p-1} \equiv 1 \pmod{p}, \text{ for } \gcd(a, p) = 1$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}, \quad p-1 \text{ is even.}$$

$$\Rightarrow a^{2^{k-1} \cdot m} \equiv \pm 1 \pmod{p}$$

- **Algorithm:** Input: an integer p (odd)

1. $p-1 = 2^k m$, where m is odd.
   choose a such that $\gcd(a,p) = 1$
2. $b \leftarrow a^m \pmod p$
3. If $b \equiv 1 \pmod p$
4. then return "p is prime".
5. For $i \leftarrow 1$ to $(k-1)$
6. If $b \equiv -1 \pmod p$
7. then return "p is prime"
8. else $b \leftarrow b^2 \pmod p$
9. return "p is composite".

- It is also probabilistic algorithm with the same property as the Fermat test stated above.

- **Example:** Let $p = 105$

$p-1 = 2^k m = 2^3 \times 13$, $k = 3, m = 13$

Let $a = 8$, $\gcd(p, a) = 1$.

Then $8^{13} \pmod{105} = 64 = b$

$b^2 \pmod{105} = 1$

$\Rightarrow$ 64 is a square root of 1

Hence 105 is not a prime by Miller-Rabin test.

Again, let $p = 49$, $p-1 = 48 = 2^4 \times 3$.

Here $m = 3$, $k = 4$

Let $a = 18$. Then $18^3 \pmod{49} = 1$

$\Rightarrow$ 49 is prime base 18.

$19^3 \bmod 49 = -1 \Rightarrow$ 49 is prime base 19.

Let $a = 5$.

Then $5^3 \pmod{49} = 27$

$27^2 \pmod{49} = 36$

$36^2 \pmod{49} = 22$

$\Rightarrow$ 49 is not a prime by Miller-Rabin test.

The discrete logarithm problem in $\mathbb{Z}_p$:

- **Problem Instance:** $I = (p, \alpha, \beta)$, where p is prime, $\alpha \in \mathbb{Z}_p$ is a primitive element, and $\beta \in \mathbb{Z}_p^*$.
- **Objective:** Find the unique integer a, $0 \leq a \leq p-2$ such that

$$\alpha^a \equiv \beta \pmod{p}$$

We will denote this integer a by $\log_\alpha \beta$.

ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$:

- Let p be a prime such that the discrete log problem in $\mathbb{Z}_p$ is intractable and let $\alpha \in \mathbb{Z}_p^*$ be a primitive element.
- Let $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ and define

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}$$

- The values p, α, β are public and a is secret.

- $K = (p, \alpha, a, \beta)$, for a (secret) random number $k \in Z_{p-1}$; define

$$e_K(x, k) = (y_1, y_2)$$

where $y_1 = \alpha^k \pmod p$

$y_2 = x \beta^k \pmod p$

- For $y_1, y_2 \in Z_p^*$, define

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \pmod p$$

- **Example:** Suppose $p = 2579$, $\alpha = 2$

$a = 765$.

$\beta = 2^{765} \bmod 2579 = 949$

- Alice wishes to send message $x = 1299$ to Bob.

Say $k = 853$ is the random integer she chooses.

Compute $y_1 = 2^{853} \bmod 2579 = 435$

$y_2 = 1299 \times 949^{853} \bmod 2579$

$= 2396$

- Bob receives $y = (y_1, y_2)$ = ciphertext.

compute $x = y_2 (y_1^a)^{-1} \pmod p$

$= 2396 (435^{765})^{-1} \bmod 2579$

$= 1299$ = plaintext.

Elliptic Curves over the Reals :

- **Definition** : Let $a, b \in \mathbb{R}$ be constants such that $4a^3 + 27b^2 \neq 0$. A non-singular elliptic curve is the set E of solutions $(x, y) \in \mathbb{R} \times \mathbb{R}$ to the equation

$$y^2 = x^3 + ax + b$$

together with a special point O called the point at infinity.

- $4a^3 + 27b^2 \neq 0 \iff x^3 + ax + b = 0$ has three distinct roots.
- $4a^3 + 27b^2 = 0 \Rightarrow$ the corresponding elliptic curve is called a singular elliptic curve.

- Suppose E is a non-singular elliptic curve. We will define '$+$' operation over E which makes $(E, +)$ an abelian group.

- Identity element : The point at infinity O is the identity element so

$$P + O = O + P = P \text{ for all } P \in E.$$

• Addition operation :

Suppose $P, Q \in E$ where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. We consider three cases

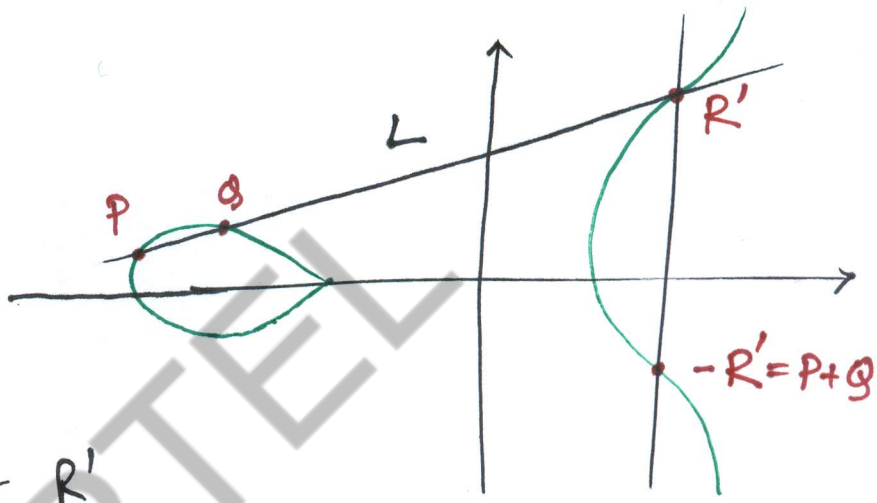
1. $x_1 \neq x_2$
2. $x_1 = x_2$ and $y_1 = -y_2$
3. $x_1 = x_2$ and $y_1 = y_2$

case 1: $x_1 \neq x_2$

Define line L through P & Q.

let L intersects E at R'.

If we reflect R' in the x-axis, then we get a point $-R'$, which we call R.



Cord and Tangent law

$$R = (x_3, y_3) = P + Q$$

where $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$ and

$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

Case 2: $x_1 = x_2$ and $y_1 = -y_2$

- We define $(x, y) + (x, -y) = O$ for all $(x, y) \in E$.
- $Q = -P$, then $P + Q = O$, i.e., O is the third point of intersection of any vertical line through P (or Q) with the curve E. Any vertical line through P (or Q) meets the curve E at infinity. This is why O is called point at infinity.
- Therefore $P = (x, y) \Rightarrow -P = (x, -y)$ are inverses with respect to the elliptic curve addition operation, i.e., $P + (-P) = O$.

Case 3: $x_1 = x_2$ and $y_1 = y_2$

- Assume that $y_1 \neq 0$, because for then we would have case 2.
- Here the line L is a tangent to E at the point P.
- If $P = (x_1, y_1) \in E$ then $P + P = (x_3, y_3)$ where $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = \dfrac{3x_1^2 + a}{2y_1}$.

- If $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$, $P \neq -Q$ then $P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \quad \text{and}$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{if } P \neq Q$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{if } P = Q$$

- $(E, +)$ is an abelian group:

1. addition is closed on the set E
2. addition is associative
3. O is an identity with respect to addition
4. every point on E has an inverse with respect to addition
5. addition is commutative.

Elliptic Curves Modulo a Prime :

- **Definition:** Let $p > 3$ be a prime. The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

where $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with a special point O called point at infinity.

- If $P = (x_1, y_1) \in E$, $Q = (x_2, y_2) \in E$ $P \neq -Q$ then $P + Q = (x_3, y_3)$ where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & \text{if } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & \text{if } P = Q \end{cases}$$

- If $P = -Q$ then $P + Q = O$.

Quadratic Residue Modulo p :

- **Definition:** Let p be an odd prime and x is an integer, $1 \leq x \leq (p-1)$. x is defined to be a quadratic residue modulo p if the congurence $y^2 \equiv x \pmod{p}$ has a solution $y \in \mathbb{Z}_p$.

- **Example:** The quadratic residues modulo 11 are $1, 3, 4, 5, 9$. Note that $(\pm 1)^2 = 1$, $(\pm 5)^2 = 3$, $(\pm 2)^2 = 4$, $(\pm 4)^2 = 5$, $(\pm 3)^2 = 9$ (all arithmatic is in $\mathbb{Z}_{11}$).

- **Problem:** An odd prime p, and an integer x such that $1 \leq x \leq (p-1)$. Is x is a quadratic residue modulo p ?

- **Euler's Criterion:** x is a quadratic residue modulo p iff $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

- Suppose z is a quadratic residue and $p \equiv 3 \pmod{4}$. Then, the two square root of z mod p are $\pm z^{(p+1)/4} \pmod{p}$.

Example :

- Let E be the elliptic curve $y^2 \equiv x^3 + x + 6$ over $\mathbb{Z}_{11}$.
- For each $x \in \mathbb{Z}_{11}$ we compute the following table to get all points of E:

x	$z = x^3 + x + 6 \pmod{11}$	quadratic residue ?	$\pm z^{(11+1)/4} \pmod{11}$ $= \pm z^3 \pmod{11}$ $= y$
0	6	no	
1	8	no	
2	5	yes	4, 7
3	3	yes	5, 6
4	8	no	
5	4	yes	2, 9
6	8	no	
7	4	yes	2, 9
8	9	yes	3, 8
9	7	no	
10	4	yes	2, 9

- E has 13 points on it including $\mathcal{O}$.
- Take a point $\alpha = (2, 7)$
- Compute $2\alpha = (2,7) + (2,7) = (x_3, y_3)$

$$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \pmod{11} = 2 \times 3^{-1} \pmod{11}$$
$$= 2 \times 4 \pmod{11}$$
$$= 8$$

$$x_3 = 8^2 - 2 - 2 \pmod{11} = 5$$

$$y_3 = 8(2-5) - 7 \pmod{11} = 2.$$

So, $2\alpha = (5, 2)$

- Next compute $2\alpha + \alpha = 3\alpha = (5,2) + (2,7)$

$\alpha = (2,7)$ $\quad 2\alpha = (5,2)$ $\quad 3\alpha = (8,3)$

$4\alpha = (10,2)$ $\quad 5\alpha = (3,6)$ $\quad 6\alpha = (7,9)$

$7\alpha = (7,2)$ $\quad 8\alpha = (3,5)$ $\quad 9\alpha = (10,9)$

$10\alpha = (8,8)$ $\quad 11\alpha = (5,9)$ $\quad 12\alpha = (2,4)$

- Thus $\alpha = (2,7)$ is a primitive element.

- ElGamal cryptosystem on E for this example:

Let, $\alpha = (2,7)$, Bob's private key is 7

Then $\beta = 7\alpha = (7,2)$

encryption: $e_K(x,k) = (k(2,7), x + k(7,2))$

where $x \in E$, $0 \le k \le 12$, and

decryption: $d_K(y_1, y_2) = y_2 - 7y_1$

where $y_2 = x + k(7,2)$, $y_1 = k(2,7)$.

Suppose $x = (10,9)$, $k = 3$.

Then $y_1 = 3(2,7) = (8,3)$

$y_2 = (10,9) + 3(7,2) = (10,9) + (3,5)$

$= (10,2)$

$\therefore e_K(x,k) = ((8,3), (10,2)) =$ ciphertext $= y$

Bob receives y and compute

$x = y_2 - 7y_1 = (10,2) - 7(8,3) = (10,2) - (3,5)$

$= (10,2) + (3,6) = (10,9)$.