Encryption Algorithms & Protocols

More Public Key Cryptography

Dr. Omar Abusada
E-mail: abossada1@gmail.com

RSA Algorithm

- Inventors, **R**ivest, **S**hamir, and **A**dleman.
- Originated By Clifford Cocks, Government Communications Head Quarter (GCHQ),
- RSA, is a Public Key Cryptography method. To generate an RSA public and private key pair, choose two large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$ and Let $\boldsymbol{N = pq}$, be the **modulus**
- Next, choose $\boldsymbol{e}$ relatively prime to the product $\boldsymbol{L=(p-1)(q-1)}$
- Finally, find $\boldsymbol{d}$ the multiplicative inverse of e modulo $\boldsymbol{L}$
- At this point, we have $\boldsymbol{N}$, which is the product of the two primes $\boldsymbol{p}$ and $\boldsymbol{q}$, as well as $\boldsymbol{e}$ and $\boldsymbol{d}$, which satisfy $\boldsymbol{ed = 1 \bmod L}$.
- Public Key is $\boldsymbol{(N,e)}$, while Private Key is $\boldsymbol{d}$

RSA Algorithm

- To encrypt with RSA, we treat the plaintext message M as a number.
- Ciphertext is calculated by raising M to the power e, modulo N, that is, $C = M^e \bmod N$
- To decrypt ciphertext C, we compute $M = C^d \bmod N$
- Note that e and N are public
- If Trudy can factor $N = pq$, she can use e to find d since $ed = 1 \bmod L$.
- Factoring the modulus breaks RSA.

Simple RSA Example

- Example of RSA
  - Select “large” primes p = 11, q = 3
  - Then N = pq = 33 and L=(p– 1)(q – 1)=(11-1)(3-1)=(10)(2) = 20
  - Choose e = 3 (relatively prime to 20)
  - Find d such that ed = 1 mod 20--------- d=1 mod 20 * 3^{-1} mod 20=1*7=7
  - We find that d = 7 works
- **Public key:**(N, e) = (33, 3)
- **Private key:** d = 7 know as “asymmetric cryptography”

Simple RSA Example

- **Public key:** (N, e) = (33, 3)
- **Private key:** d = 7
- Suppose message M = **8**
- Ciphertext C is computed as
  - $\boldsymbol{C = M^e mod\ N}$ = **8**^{3} = 512= 17 mod33
- Decrypt C to recover the message M by
- $\boldsymbol{M = C^d mod\ N}$ = 17^7 = 410,338,673 mod 33

  = 12,434,505 *33 + **8** = **8** mod 33

- **Public key:** (N, e) = (33, 3)
- **Private key:** d = 7
- Suppose message M = **6**
- Ciphertext C is computed as
  - $\boldsymbol{C = M^e mod\ N}$ = **6**^{3} = 216= 18 mod 33
- Decrypt C to recover the message M by
- $\boldsymbol{M = C^d mod\ N}$ = 18^7 = 612,220,032 mod 33

  = 18552122 *33 + **6** = 6 mod 33

Diffie-Hellman

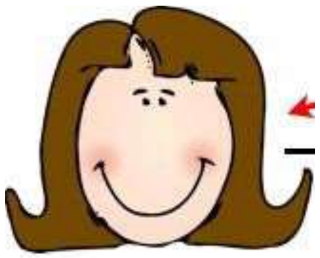
- The Diffie-Hellman (DH) key exchange algorithm, or DH for short, was invented by Malcolm Williamson of GCHQ.
- Based on discrete log problem:
  - o Given: **g, p,** and $\mathbf{g^k}$ **mod p**
  - o Find: exponent **k**
- Let **p** be prime, let **g** be a **generator**, and both are public.
- For any **x** Є{1,2,…,p-1} there is an exponent **n** such that $\mathbf{x = g^n}$ **mod p**
- Alice selects her private value **a**
- Bob selects his private value **b**

Diffie-Hellman

- Alice sends $\mathbf{g^a \bmod p}$ to Bob
- Bob sends $\mathbf{g^b \bmod p}$ to Alice
- Both compute shared secret, $\mathbf{g^{ab} \bmod p}$
- Shared secret can be used as symmetric key
- Suppose Bob and Alice use **Diffie-Hellman** to determine symmetric key $\mathbf{K = g^{ab} \bmod p}$
- Trudy can see $\mathbf{g^a \bmod p}$ and $\mathbf{g^b \bmod p}$
  - But… $\mathbf{g^a g^b \bmod p = g^{a+b} \bmod p \neq g^{ab} \bmod p}$
- If Trudy can solve discrete log problem, she can find a or b

Diffie-Hellman

- Public: **g** and **p**
- Private: Alice's exponent **a**, Bob's exponent **b**



Alice **a**

$$\text{Alice} \xrightarrow{\mathbf{g^a \bmod p}} \text{Bob}$$

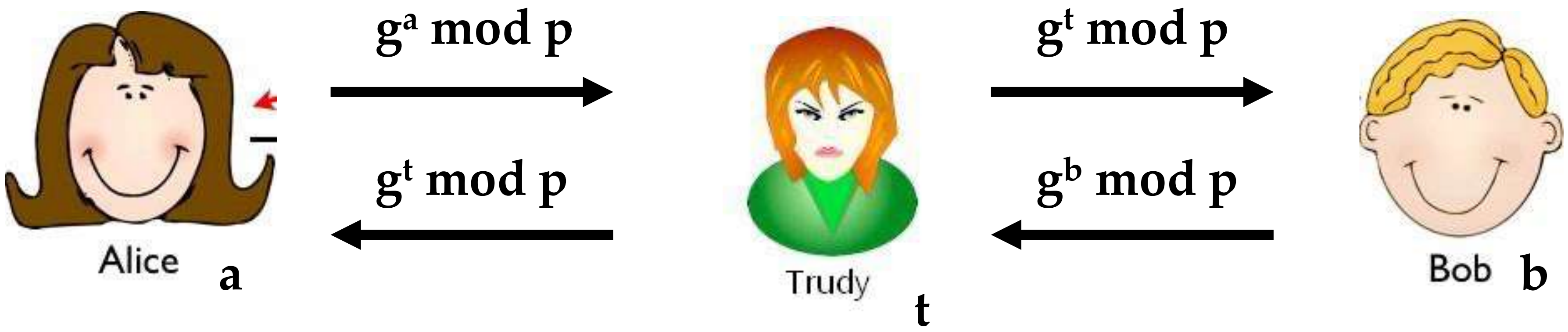
$$\text{Alice} \xleftarrow{\mathbf{g^b \bmod p}} \text{Bob}$$

Bob **b**

- Alice computes $(g^b)^a = g^{ba} = g^{ab} \bmod p$
- Bob computes $(g^a)^b = g^{ab} \bmod p$
- Use $K = g^{ab} \bmod p$ as symmetric **key**

Diffie-Hellman

- Subject to man-in-the-middle (MiM) attack



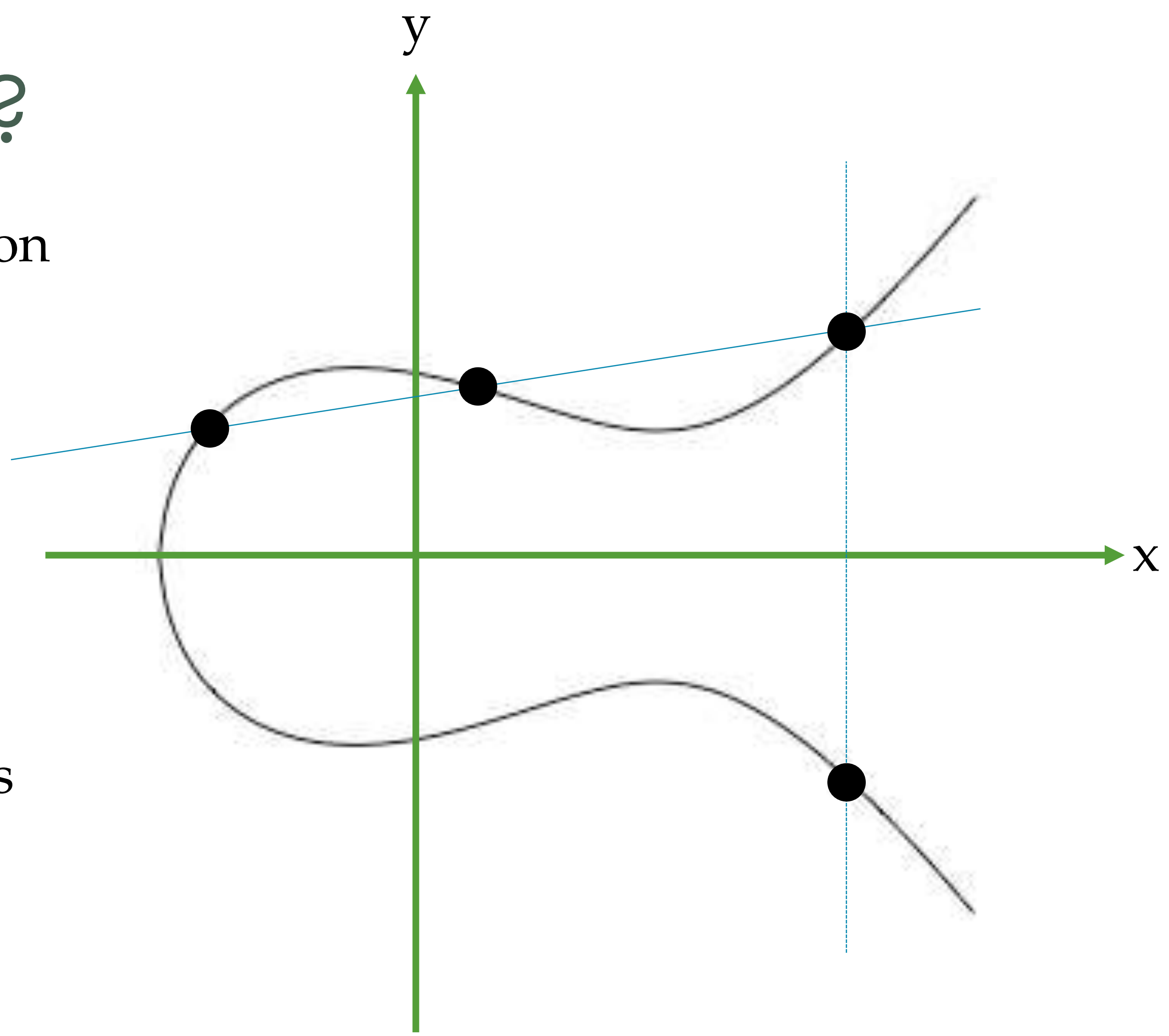
- Trudy shares secret g^{at} **mod p** with Alice
- Trudy shares secret g^{bt} **mod p** with Bob
- Alice and Bob don't know Trudy exists!

Elliptic Curve Crypto (ECC)

- "Elliptic curve" is not a cryptosystem
- Elliptic curves are a different way to do the math in public key system
- Elliptic curve versions DH, RSA, etc.
- Elliptic curves may be more efficient
  - Fewer bits needed for same security
  - But the operations are more complex

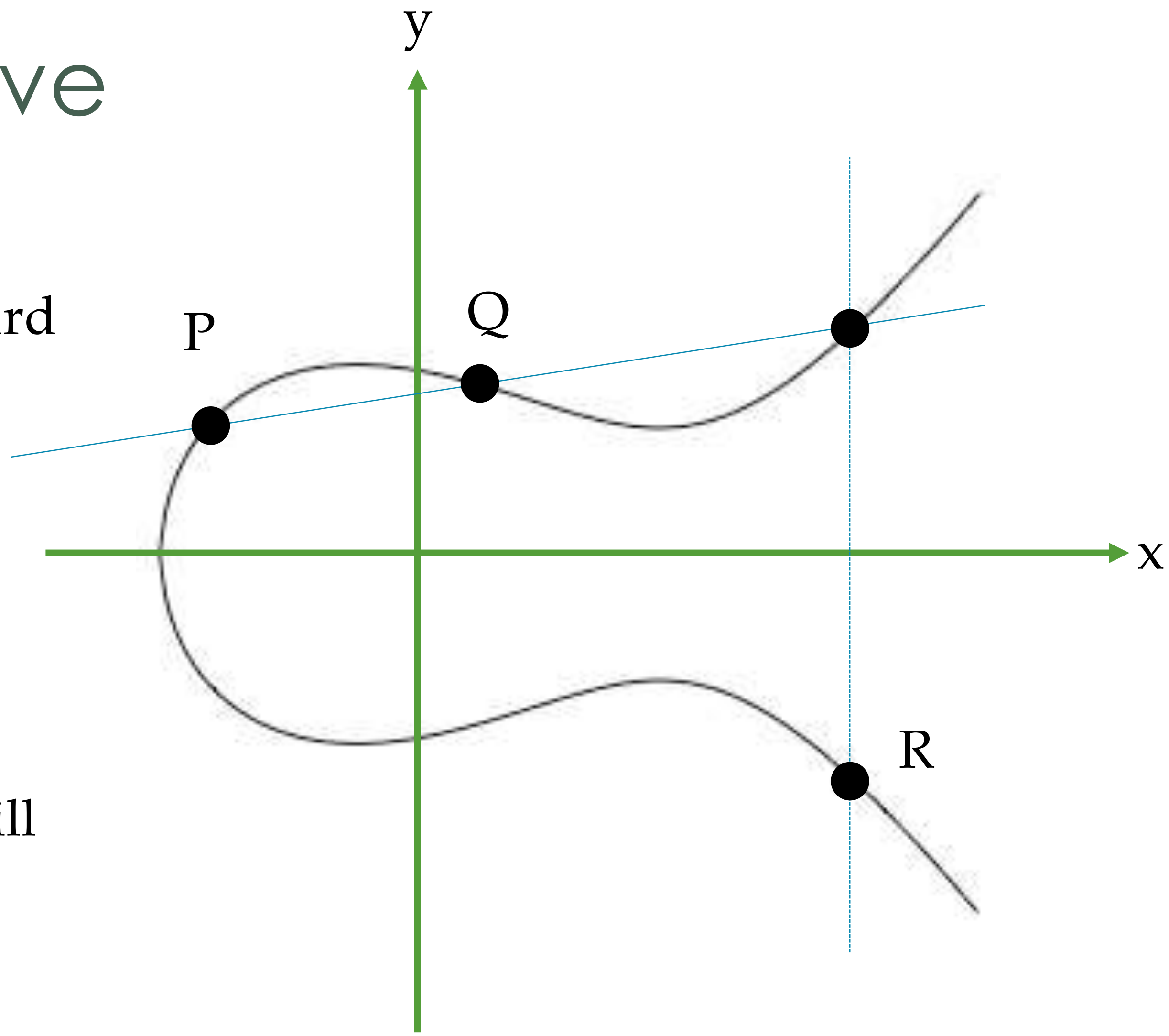
What is an Elliptic Curve?

- An elliptic curve E is the graph of an equation of the form
- $y^2 = x^3 + ax + b$
- Also includes a "point at infinity"
- What do elliptic curves look like?
- Elliptic curve is a symmetrical around x-axis



Operation on Elliptic Curve

- Say $P = (x_1, y_1), Q = (x_2, y_2)$
- We can compute the coordinate for the third point R as: $R = P + Q$
- $R = P + Q, (x_3, y_3) = (x_1, y_1)+(x_2, y_2)$
- Draw a line through P and Q to obtain third point of intersection
- Mirror the intersection point along x-axis will define the point R



Points on Elliptic Curve

x	$x^3 + 2x + 3 \pmod 5$
0	no solution
1	1
2	0
3	1
4	0

y	$Y^2 \pmod 5$
0	0
1	1
2	4
3	4
4	1

- Consider $y^2 = x^3 + 2x + 3$, that means
- $y^2(mod\ P) = x^3 + 2x + 3(mod\ P), P = 5$
- $y^2(mod\ 5) = x^3 + 2x + 3(mod\ 5)$

- Consider $P = 5$, that means Prime numbers should $0,1,2, \ldots . P_{n-1}$
- $x = 0 \quad \rightarrow \quad y^2 = 3 \quad \rightarrow$ no solution$(mod\ 5)$
- $x = 1 \quad \rightarrow \quad y^2 = 6 = 1 \quad \rightarrow$ y=1,4 $(mod\ 5)$
- $x = 2 \quad \rightarrow \quad y^2 = 15 = 0 \quad \rightarrow$ y= 0 $(mod\ 5)$
- $x = 3 \quad \rightarrow \quad y^2 = 36 = 1 \quad \rightarrow$ y= 1,4 $(mod\ 5)$
- $x = 4 \quad \rightarrow \quad y^2 = 75 = 0 \quad \rightarrow$ y= 0 $(mod\ 5)$
- Then points on the elliptic curve are (1,1) (1,4) (2,0) (3,1) (3,4), (4,0)

Elliptic Curve Math

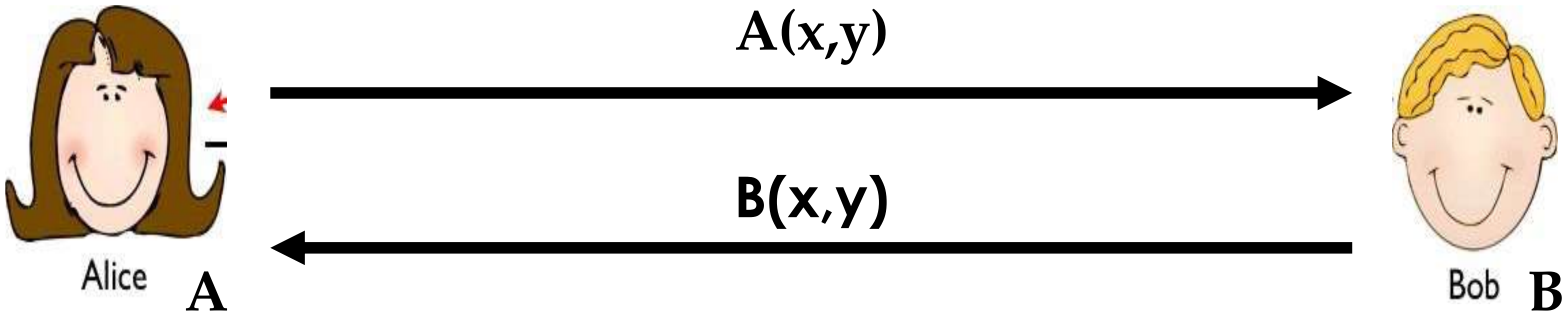
- Addition on: $y^2 = x^3 + ax + b(mod\ P)$
- $Suppose\ that\ P_1 = (x_1, y_1)\ and\ P_2 = (x_2, y_2)$
- $P_1 + P_2 = P_3 = (x_3, y_3)\ where$
- $x_3 = m^2 - x_1 - x_2(mod\ P)$
- $y_3 = m(x_1 - x_3) - y_1\ (mod\ P)$
- $where\ m = \begin{cases} (y_2 - y_1)\ .\ (x_2 - x_1)^{-1}\ \ mod\ P & if\ \ P_1 \neq P_2 \\ (3x_1^2 + a\ ).\ (2y_1)^{-1} mod\ P & if\ \ P_1 = P_2 \end{cases}$
- $Spicial\ cases\quad (1)\ \ if\ \ \ m\ is\ \infty\ \ then\ \ P_3\ \ is\ \ \infty \qquad (2)\quad \infty + P = P\ \ \ for\ all\ \ \ P$

Elliptic Curve Addition

- According to $y^2(mod\ 5) = x^3 + 2x + 3(mod\ 5)$,
- we get the following points: (1,1) (1,4) (2,0) (3,1) (3,4), (4,0),
- Let's apply the previous algorithm to find the point P_3.
- $where\ P_3 = (x_3, y_3) = (1,4) + (3,1)$
- $m = (1-4) * (3-1)^{-1} = -3 * 2^{-1} = 2(3) = 6 = 1\ mod\ 5$
- $x_3 = 1 - 1 - 3 = -3 = 2\ mod\ 5$
- $y_3 = 1(1-2) - 4 = 0\ mod\ 5$
- $On\ the\ Elliptic\ Curve, (1,4) + (3,1) = (2,0)$

ECC Diffie-Hellman

- **Public:** Elliptic curve and point (x,y) on curve
- **Private:** Alice's **A and** Bob's **B**



- Alice computes A(B(x,y))
- Bob computes B(A(x,y))
- These are the same since AB = BA

EX: ECC Diffie-Hellman

- Public: Curve $y^2 = x^3 + 2x + 2(mod\ 17), and\ the\ Point\ G = (5{,}1)"Generator“$
- 2G=G+G (same point)
- **Alice's private: A = 4** → b = 9 $y^2 = x^3 + 7x + 9\ (mod\ 37)$
- **Bob's private: B = 7** → a = 9 $y^2 = x^3 + 5x + 7\ (mod\ 37)$
- Calculate $m = (3x_G^2 + a\ ).\ (2y_G)^{-1} mod\ P$ $since\ \ P_1 = P_2, G = G$
- $m = \left(3 * 5^2\ \ +2\ \right) * \ (2 * 1)^{-1} mod\ 17 = 77 * (2)^{-1}\ mod\ 17 = 9 * 9\ mod\ 17 = 13\ mod\ 17$
- $x_{2G} = m^2 - x_G - x_G(mod\ P) = 13^2 - 5 - 5\ mod\ 17 = 6\ mod\ 17$
- $y_{2G} = m(x_G - x_{2G}) - y_G\ (mod\ P) = 13(5-6) - 1\ (mod\ 17) = -14\ mod\ 17 = 3\ mod\ 17$

2G=(6,3)

... Thank you ...