Elliptical Curve Cryptography

Rishi Nair
Mentor: Adrian She

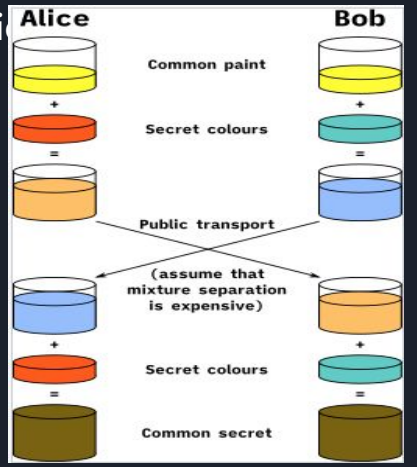
Cryptography Overview

- Cryptography is the practice and study of techniques for secure communication.
- Cryptography is necessary for the exchange of sensitive information.
- How do we encrypt, send, receive and decrypt information send over the internet?
- A "key" can encrypt or decrypt data. Key generation and exchange is the process of giving the receiver a key that can be used to decrypt data send by a sender.
- Public-key cryptography is a common cryptography system. The sender and the receiver will have a public (which may be known to others) and a private key (which is not known by anyone except the owner).
- For the sender and receiver to obtain the same "common secret" the keys must be exchanged somehow.
- One such method is known as the Diffie–Hellman key exchange.

Diffie-Hellman Key Exchange

Example of Implementation with Factorization Key Generation:

1. Person X and Y publicly agree to use a modulus p = 23 and base g = 5 (whi is a primitive root modulo 23).
2. X chooses a secret integer a = 4, then sends Y A = g^a mod p
   - A = 5^4 mod 23 = 4
3. Y chooses a secret integer b = 3, then sends X B = g^b mod p
   - B = 5^3 mod 23 = 10
4. X computes s = B^a mod p
   - s = 10^4 mod 23 = 18
5. Y computes s = A^b mod p
   - s = 4^3 mod 23 = 18
6. X and Y now share a secret (the number 18).



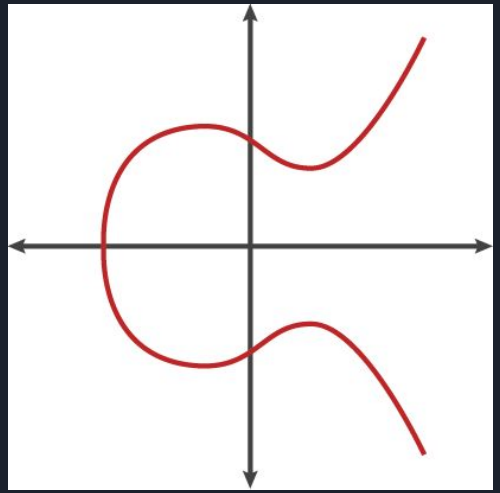
Obtaining a "secret color" using the diffie-hellman key exchange

The secret number can now be used as a "master key" by either X or Y to encrypt and decrypt information.

Function must be a "trapdoor function" and f(g(x)) = g(f(x)).

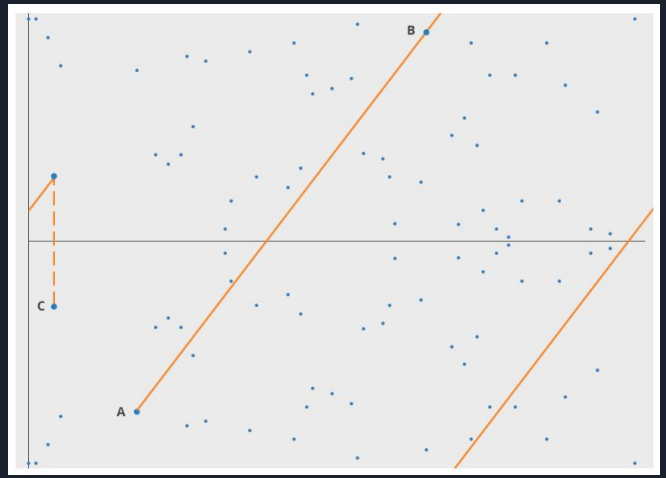
Elliptical Curve Cryptography Overview

- Elliptical curve cryptography is a public key cryptosystem (contains key generation, encryption and decryption algorithms).
- Trapdoor function: Math function behind the public key cryptosystem. You can take a given value "A" and use the trapdoor function to get "B." But it is very difficult/complex to get from "B" back to "A."
- ECC is generally more secure than RSA cryptosystems (the most commonly used trapdoor function). A 256 bit key size using ECC has the same level of security as a 3072 bit key using RSA. This goes up exponentially. The National Security Agency states that a 384 bit ECC key is secure enough to transfer highly sensitive information.
- Elliptical Curve keys are generated using an elliptical curve (on the right) hence its name



Elliptical Curve Key Generation

- An elliptical curve is a plane curve over any field (finite fields are used for ECC cryptography) which consists of points satisfying the equation: $y^2 = x^3 + ax + b$ along with a distinguished point at infinity (the identity element). An elliptical curve is symmetrical along the x axis. If you draw a straight line through any point in the graph, the line will not intersect that curve at more than 3 points.
- Let A, B, C, D, … Z, be points on the elliptical curve, where A is the starting point and Z is the ending point. Let $\cdot$ be the binary operation of the elliptical curve group. $A \cdot B = C$ is true if we can draw a line through A and B, intersect the curve at point C.
- Algorithm: $A \cdot B = C$. Reflect C along the x-axis to obtain point D. $A \cdot D = E$. Reflect point E along the x-axis to obtain point F.



Elliptical Curve Key Generation

- We can repeat the algorithm to get multiple points. We can set a max x and y value to keep everything inside a domain and range (reducing complexity of the scheme). If the line in the dot product operator goes outside the "box," it "resets.". As we increase the key size (in bits) of the ECC cryptosystem, we are increase the space in which we can work with.
- The private key is "n" which is the number of times you use the dot operation. The public key is the curve, the starting point and the ending point.
- This is a trapdoor function. If you are given only the starting point, and ending point, and the curve (the public information), it is extremely difficult to find out "n" (the private information).
- There is a lot of research on which elliptical curve is the best to use (secure and efficient) for key generation. The US National Institute of Standards and Technology recommends 15 different elliptical curves, each of which works best with different bit sizes.

Thank You