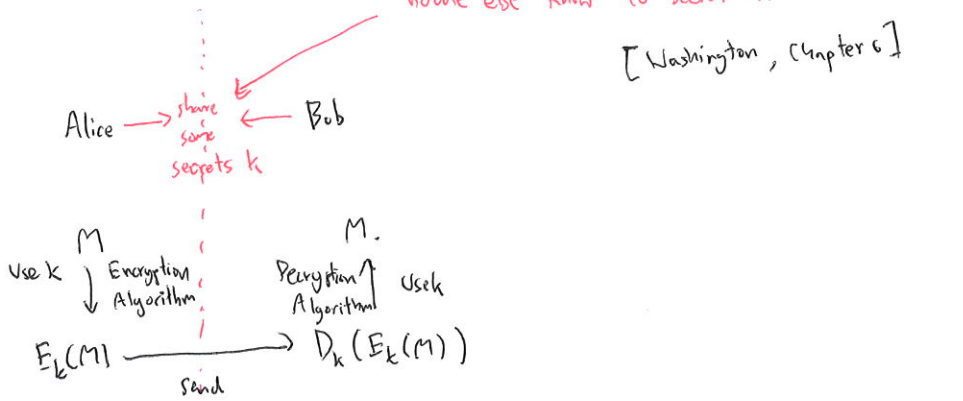
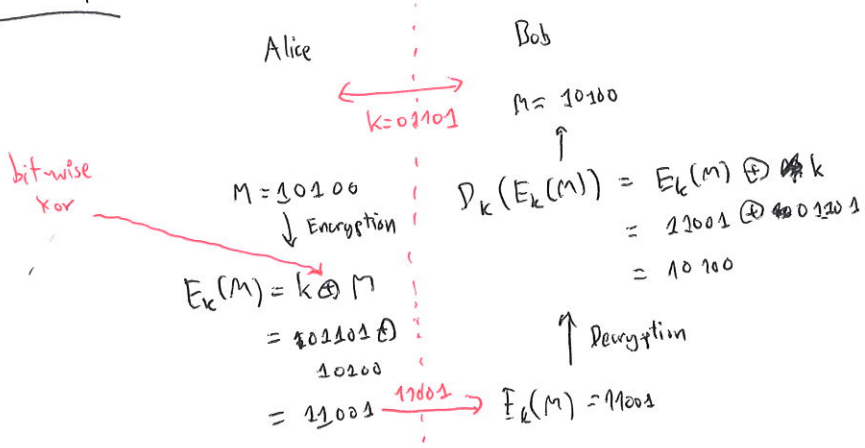
Private Key Cryptography

[Washington, Chapter 6]



One-time pad

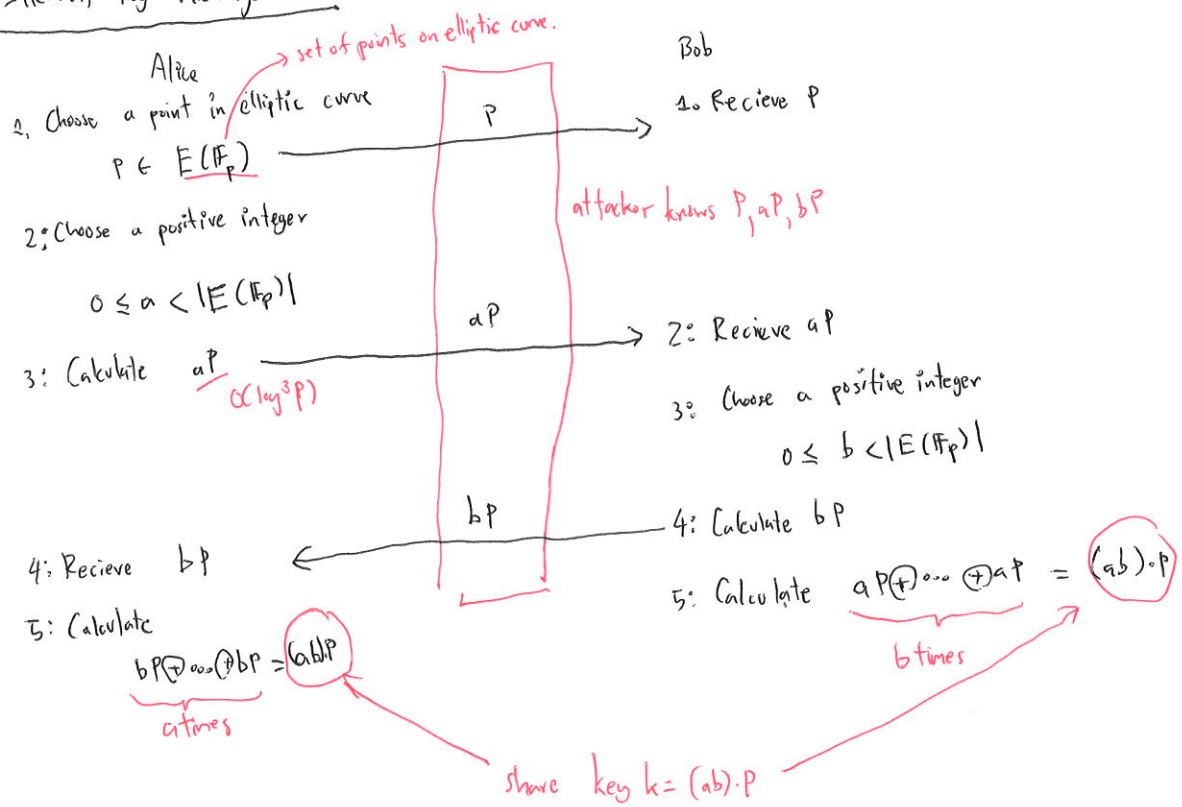


- One-Time Pad is known to be costly and weak.
- Currently, Advanced Encryption Scheme (AES) is the most commonly used cryptosystem.

Problem How can Alice and Bob share the key k to each other? → Key Exchange Protocol.

Diffie-Hellman Key Exchange Protocol

[Washington, Chapter]



Diffie-Hellman Problem

Input : P, aP, bP

Calculate : $(ab)P$

equivalent

Discrete Logarithm Problem

Input : P, aP

Calculate : a

Large when $p \approx 2^{256}$

very hard problem

not possible to have algorithm faster than $O(\sqrt{p})$

Algorithms for Discrete Logarithm Problem : Baby step, Giant step

Input : P, Q

Find : a such that $a \cdot P = Q$

$N = \sqrt{|E(\mathbb{F}_p)|}$ (maximum value for a) → $O(N)$

1. Calculate $S = \{P, 2P, 3P, \dots, N \cdot P\}$ (baby step)
2. Check if any in S is equal to Q. If yes, we have a.

$\Leftarrow Q \oplus \neg(NP)$. If $\Rightarrow bP = Q \oplus (\neg NP)$

↳ the entry that we hit.

$bP \oplus NP = Q \oplus (\neg NP) \oplus (NP)$

$Q = \underbrace{(b+N)}_{a} \cdot P$

Check if any in S is equal to $Q \oplus \neg(2N \cdot P)$. $\Rightarrow bP = Q \oplus (\neg 2N \cdot P)$

$bP \oplus 2N \cdot P = Q \oplus (\neg 2N \cdot P) \oplus (2N \cdot P)$

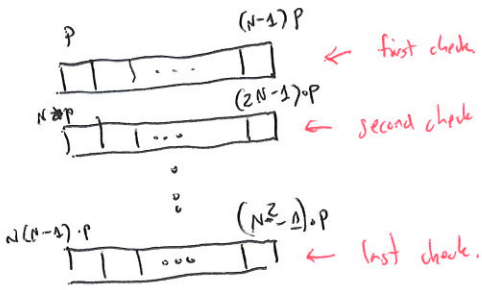
$\underbrace{(b+2N)}_{a} \cdot P = Q$

⋮

Check if any in S is equal to $Q \oplus \neg((N-1)N \cdot P)$ $\Rightarrow$ $Q = ((N-1)N + b) \cdot P$.

Any of these cases must be satisfied.

$O(N)$



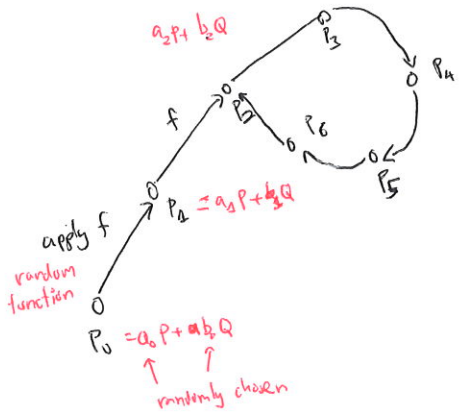
Time Complexity $O(N) = O(\sqrt{|E(\mathbb{F}_p)|})$ ← may be doable when $p \approx 2^{128}$

Memory Complexity $O(N) = O(\sqrt{|E(\mathbb{F}_p)|})$ ← not doable even when $p \approx 2^{64}$

[Washington, Chapter 5]

Pollard's ρ Method

Idea



$P_2 = P_7$

$a_2P \oplus b_2Q = a_7P \oplus b_7Q$

$a_2P \oplus b_2Q \oplus -b_2Q \oplus -a_7P$

$= a_7P \oplus b_7Q \oplus -b_2Q \oplus -a_7P$

$(a_2 - a_7) \cdot P = (b_7 - b_2)Q$

We can solve this equation to obtain $P = a \cdot Q$ (explained later)

- We will be back to the visited point after $O(\sqrt{|E(\mathbb{F}_p)|})$ applications of f.
- But, how to check if a particular point → store all the points will consume $O(\sqrt{|E(\mathbb{F}_p)|})$ ☹

Idea

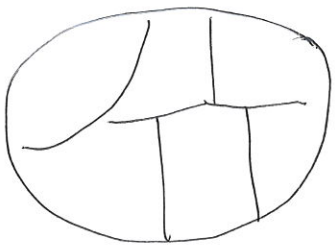
Use fast and slow kangaroos

fast: move 2 hops, apply f for 2 times

slow: move 1 hop, apply f for 2 times

What is function f?

- To guarantee that the visited point is found in $O(\sqrt{|E(\mathbb{F}_p)|})$, f has to be random.
- It is hard to have the random function, as we need to have the same output for the same input. (Then, we have to store f(P) for many point P.)



Divide $E(\mathbb{F}_p)$ into 20 pieces $S_1, \ldots, S_{20}$

For $P_i \in S_j$, $f(P_i) = P_i \oplus a_j P \oplus b_j Q$

a_j, b_j: random number

Algorithm

random numbers; slow kangaroo; fast kangaroo

1: $P_0 \leftarrow a_0P + b_0Q$, $R \leftarrow P_0$ and $S \leftarrow P_0$

2: P_0

$R \leftarrow f(R)$, $Q \leftarrow f(f(R))$

Until $R = S$

3: Suppose that $R = a_{i_1}P \oplus b_{i_1}Q$

$S = a_{i_2}P \oplus b_{i_2}Q$

Solve $a_{i_1}P \oplus b_{i_1}Q = a_{i_2}P \oplus b_{i_2}Q$ to have

$Q = \bigcirc P$

Example $p = 1093$ $A = B = 1$ $E(\mathbb{F}_{1093}) = \{(x,y) \in \mathbb{F}_{1093}^2 : y^2 \equiv y = x^3 \oplus x \oplus x \oplus 1\}$

$|E(\mathbb{F}_{1093})| = 1067$

Input: $P = (0,1)$, $Q = (413, 957)$.

[We want to find a such that $(413, 957) = a(0,1)$]

$$f(x,y) = \begin{cases} (x,y) \oplus 4P \oplus 3Q & \text{when } x \equiv 0 \bmod 3 \\ (x,y) \oplus 9P \oplus 17Q & \text{when } x \equiv 1 \bmod 3 \\ (x,y) \oplus 14P \oplus 6Q & \text{when } x \equiv 2 \bmod 3 \end{cases}$$

1: $P_0 = 3P \oplus 5Q = (326, 69) = R = S$ → random number

Iteration 1 $R = f(R) = (326, 869) \oplus 14(0,1) \oplus 6(413, 957) = (727, 589)$

$S = f(f(S)) = f((727, 589)) = (727, 589) \oplus 9(0,1) \oplus 17(413, 957)$

$= (560, 365)$

$R = (3P + 5Q) \oplus 14P \oplus 6Q = 22P \oplus 11Q$

$S = (22P \oplus 11Q) \oplus 9P \oplus 17Q = 31P \oplus 28Q$

Iteration 2 $R = (727, 587) = 31P \oplus 28Q$

$S = (473, 903) = 69P \oplus 40Q$

⋮

Iteration 53 $R = (71, 338) = 620P \oplus 557Q$ $S = (71, 338) = 1217P \oplus 1131Q$

$620P \oplus 557Q = 1217P \oplus 1131Q$ [$|E(\mathbb{F}_{1093})| = 1067$, $1067P = e$ for any P.]

$620P \oplus 557Q = 1067P \oplus 150P \oplus 1067Q \oplus 64Q$ ($1067P = e$, $1067Q = e$)

$620P \oplus 557Q = 150P \oplus 64Q$

$620P \oplus 557Q \oplus 510Q \oplus -150P = 150P \oplus 64Q \oplus 510Q \oplus -150P$

$1067Q = e$

$k \cdot 470P = k \cdot 574Q$

$k \cdot 470P = [1067n + 1]Q$

Bonus Question

Solve Diophantine's equation $1067n + 1 = 574k$ when k, n are integers,

Ans $k = 303$ $n = 163$

$(303 \cdot 470)P = [1067 \cdot 163 + 1]Q$

$142410P = Q$

$[\#133 \cdot 1067 + 499]P = Q$

$499P = Q$

$a = 499$.

17