DAA IT300 Project
Cracking Knapsack Cryptosystem- LLL algorithm

S.Shushal - 181IT239 - 6362897847

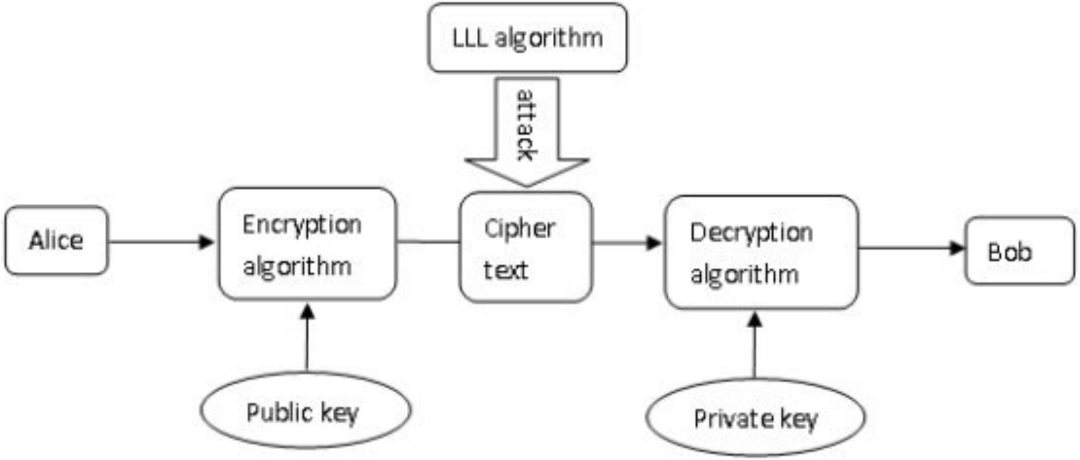
Sarthak Laghate - 181IT141 - 6264857849

Jay Agrawal - 181IT219 - 8149918273

Sheel Lohia - 181IT143 - 9973947040

Introduction

- It is an asymmetric-key cryptosystem, meaning that two keys are required for communication: a public key and a private key.
- Furthermore, the public key can be known widely and used only for encryption, and the private key is known only by the owner and used only for decryption.



Introduction

There are four main processes in knapsack cryptosystem:

- Key generation
- Encryption
- Decryption
- Cracking (by LLL Algorithm - without using the private key).

Key generation

- According to the Knapsack cryptosystem, the first step in encryption is to generate a public key by given private key. The private key is supposed to be a super-increasing 8 sequence a1, a2, … , an

  satisfying that $a_i > \sum_{j=1}^{i-1} a_j$

  Here we set n equals to 7 because the length of ASCII binary code of alphabets are 7 digits. Set multiplier m and modular w.

  m,w are integers and satisfy that m >2a , gcd(m,w) = 1

- Then the public key can be calculated as. As the public key is not a super-increasing sequence, it is not easy to solve the Knapsack problem by using the public key.

$$b_i \equiv wa_i \pmod{m},\ 0 \le b_i < m.$$

Encryption

- After gaining the public key, transfer the text that need to be encrypted into binary digits.
- For example, ‘A’ can be transferred as ‘1000001’ in binary digits. Take xij as the jth digit of the ith letter in text.
- Then the ith letter can be encrypted as follows,

$$s_i = b_1 x_{i1} + b_2 x_{i2} + \cdots + b_7 x_{i7}$$

- Subsequently, the cypher text will be sent to receiver who already has the private key. During this situation, the cypher text and public key maybe captured by other codebreakers.

Decryption

After the receiver gains the ciphertext, the main purpose is to transfer the problem into a solvable Knapsack problem. First step is to calculate w−1, the modular inverse of w with respect to the modulus m.

For every cypher text Si , we have

$$t_i = w^{-1} s_i (mod\ m)$$

$$= w^{-1} \sum_{j=1}^{7} b_i x_{ij}\ (mod\ m)$$

$$= w^{-1} \sum_{j=1}^{7} wa_i (mod\ m) x_{ij}\ (mod\ m)$$

$$= \sum_{j=1}^{7} a_i x_{ij}\ (mod\ m) = \sum_{j=1}^{7} a_i x_{ij}$$

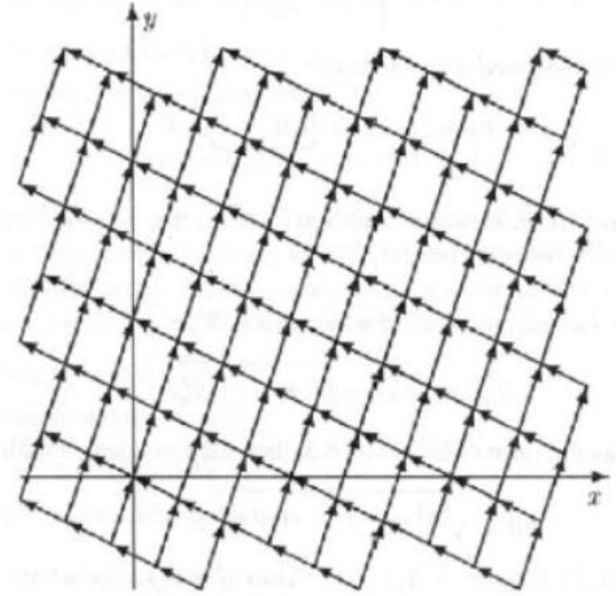
Cracking

- As for the codebreakers who capture the cypher text during transmission. The LLL reduction algorithm can be used to decrypt the ciphertext without private key. Firstly, by given ciphertext s and public key a, we generate a matrix.

$$M_i = \begin{bmatrix} I_{7\times 7} & 0_{7\times 1} \\ a_{1\times 7} & -s_i \end{bmatrix}.$$

- Because the basis is relatively long, by using LLL algorithm can reduce the length of basis. The LLL Algorithm outputs a matrix Mi', consisting of short vectors in the lattice spanned by the columns of the matrix Mi.

$$c_0 = \binom{-1}{1} \quad and \quad c_1 = \binom{1}{2}.$$



The Basis of lattice is 2 i.e
Two independent vectors -1i+1j and 1i+2j formed the lattice

- Find a column in matrix $Mi\,'$ that only consists of 1 and 0 or -1 and 0 (LLL algorithm probably generates an inverse reduced basis).
- The first seven digits are the binary code of the ith alphabet. Finally, convert the binary code into character, we gain the original text.

Result

The reduced matrix is:

-2	0	-1	1	1	1	0	0
1	-2	0	0	0	0	0	1
0	1	-2	1	0	-1	0	0
0	0	1	0	1	-1	-1	-1
0	0	0	0	1	1	1	0
0	0	0	-1	0	1	-1	0
0	0	0	1	1	0	-1	2
0	0	0	1	0	1	0	-1

The LLL decryption text is: M

The reduced matrix is:

-1	-1	-1	0	0	0	0	1
0	1	-1	1	-1	-1	0	0
1	-1	0	0	0	-1	0	0
0	0	0	0	-1	1	-1	0
0	0	0	0	0	0	1	2
0	0	0	-1	-1	0	1	-1
1	-1	-1	0	0	1	1	0
0	0	0	1	0	0	1	0

The LLL decryption text is: a

The reduced matrix is:

0	-2	0	-1	0	0	1	0
-1	1	-1	-1	0	0	0	0
0	0	1	-1	-1	-1	-1	0
1	0	-1	0	-1	1	-1	0
1	0	-1	-1	0	0	1	1
0	0	0	0	-1	-1	1	0
0	0	0	0	0	1	0	2
0	0	0	0	0	1	1	-1

The LLL decryption text is: t

The reduced matrix is:

-1	-1	-1	0	0	0	1	0
0	1	-1	-1	1	0	0	1
1	-1	0	-1	0	0	0	0
1	-1	-1	2	-1	0	0	-1
0	0	0	0	0	1	2	0
0	0	0	0	-1	1	-1	0
0	0	0	0	1	0	0	2
0	0	0	0	1	1	0	-1

The LLL decryption text is: h >>

Conclusion

-Comparing our project to referred papers such as them using brute force , dynamic programming our project is very efficient.

-We have solved the disadvantages they have faced while implementing the attacker.

-Our project accepts any characters including special characters and large length of text can be deciphered very quickly.