CS641

Modern Cryptology

Indian Institute of Technology, Kanpur

Group Name: The_Kryptonians

Maulik Singhal (190489), Pranshu Gaur (200703), Maryam Raza Khan (190488)

End Semester Examination

Submission Deadline:
May 5, 2022, 11:55hrs

Solution 1

Lattice

We prove that the Lattice generated by $\hat{L}$ is same as Lattice generated by $n \cdot R$

Claim 1.1 : If $U \in \mathbb{Z}^{n \times n}$ is a unitary matrix that is det $U = 1$, then two matrices M and M' generate the same lattice if $M = U \cdot M'$

Proof : To prove this we make use of the fact that if U is a Unitary Matrix then, U^{-1} is also a Unitary Matrix.

First let us assume that $M = U \cdot M'$. In particular, both U and U^{-1} are integer matrices, and $M = U \cdot M'$ and $M' = M \cdot U^{-1}$ It follows that $\mathcal{L}(B) \subseteq \mathcal{L}(C)$ and $\mathcal{L}(C) \subseteq \mathcal{L}(B)$, i.e., the two matrices B and C generate the same lattice.

Now assume B and C are two bases for the same lattice $\mathcal{L}(B) = \mathcal{L}(C)$ Then, by definition of lattice, there exist integer square matrices V and U such that $B = C \cdot U$ and $C = B \cdot V$. Combining these two equations we get $B = B \cdot V \cdot U$, or equivalently, $B \cdot (I_n - V \cdot U) = O$. Since B is non-singular, it must be $I_n - V \cdot U = O$, i.e., $V \cdot U = I_n$ and hence $|\det U| = 1$. Thus, det $U = 1$, Unitary Matrix is a solution. The claim holds

Claim 1.2 :As a Rotation Matrix 'R' has an orthonormal basis, the matrix $n \cdot R$ will have an orthogonal basis of n vectors each of length n.

Proof : To see this, let $\{b_1, b_2, .., b_n\}$ be an orthonormal basis of R, therefore $\langle b_i, b_j \rangle = 0$ $\forall i \neq j$ and $\langle b_i, b_j \rangle = 1$ if $i = j$

Now, if the matrix is $n \cdot R$, then the basis is $\{n \times b_1, n \times b_2, .., n \times b_n\}$ and let $a_i = n \times b_i$, then $\langle a_i, a_j \rangle = n^2 \langle b_i, b_j \rangle = 0$ $\forall i \neq j$ and $\langle a_i, a_j \rangle = n^2 \langle b_i, b_j \rangle = n^2$ if $i = j$. Therefore the basis is orthogonal and length of each vector is $\|b_i\| = \sqrt{\langle b_i, b_i \rangle} = n$

Thus Lattice generated by $n \cdot R$ has a basis consisting of n orthogonal vectors, each of length n. The Claim holds.

By Claim 1.1, Lattice generated by $U \cdot n \cdot R$ and by $n \cdot R$ are same, as U is a Unitary Matrix.

But, $U \cdot n \cdot R = U \cdot n \cdot I_n \cdot R = U \cdot L \cdot R = \hat{L}$

Therefore, Lattice generated by $\hat{L}$ has an orthogonal basis of n vectors with length of each vector = n.

Decryption

We show that the decryption works properly by computing '**m**' as stated in the question.

Given the Output Vector '**c**' that is the same as '$v \cdot \hat{L} + m$' , substituting $\hat{L}$ as $U \cdot L \cdot R$ and L as $n \cdot I$ we have $c = n(v \cdot U \cdot R) + m$

Now the vector '**d**' is calculated as $d = c \cdot R^T$

Each entry of the vector 'd' is reduced by taking modulus n in the following way:

$$f(a_i) = \begin{cases} a_i \pmod{n} - n & \textbf{if } a_i \pmod{n} > \frac{n}{2} \\ a_i \pmod{n} & \textbf{otherwise} \end{cases}$$

Here a_i is an element of the vector 'd', and the newly formed vector with elements $f(a_i)$ is named as $\hat{d}$

We notice that the term '$n(v \cdot U \cdot R) \cdot R^T$' $\equiv 0 \pmod{n}$ and hence,

$\hat{d} = f(m \cdot R^T)$ where f applied to the matrix means that f is applied to each element separately.

Claim 2.1 : Each element of the matrix R lies in $[-1, 1]$

Proof : Let the elements of R be a_{ij}

Now since $R \cdot R^T = I_n$, by comparing the diagonal elements we have

$$\sum_{j=1}^{n} a_{ij}^2 = 1 \quad \forall i \in \{1, 2, ..., n\}$$

Therefore $-1 \leq a_{ij} \leq 1 \quad \forall i, j \in \{1, 2, ..., n\}$

Claim 2.2 : $f(m \cdot R^T) = m \cdot R^T$ (where f applied to the matrix means that f is applied to each element separately)

Proof : We prove that each element of the vector $m \cdot R^T$ lies in $(-\frac{n}{2}, \frac{n}{2})$ and hence each element modulo n returns the same element.

Here we use the fact that each entry of the vector m is either 0 or 1.

Let the elements of m be m_i, R^T be a_{ij} and $m \cdot R^T$ be b_j

Now by comparing the terms we have,

$$b_j = \sum_{i=1}^{n} m_i \times a_{ij} \quad \forall j \in \{1, 2, ..., n\}$$

$$\Rightarrow b_j \leq \sum_{i=1}^{n} 1 \times a_{ij} = \sum_{i=1}^{n} a_{ij} \quad (\text{As } m_i \in \{0,1\})$$

Now, as $\sum_{i=1}^{n} a_{ij}^2 = 1$; $\sum_{i=1}^{n} a_{ij}$ will be maximum (or minimum) when each a_{ij} is equal to $\frac{1}{\sqrt{n}}$ (or $\frac{-1}{\sqrt{n}}$, respectively) because the sum will maximize (or minimize), when the elements are equal and positive (or negative), due to the symmetry of the equation.
Hence, $-\sqrt{n} = \sum_{i=1}^{n} \frac{-1}{\sqrt{n}} \leq b_j \leq \sum_{i=1}^{n} \frac{1}{\sqrt{n}} = \sqrt{n}$
Therefore $-\sqrt{n} \leq b_j \leq \sqrt{n} \quad \forall j \in \{1, 2, ..., n\}$

If n is small (< 10), security is very weak. Therefore we assume large n.
Hence, $\forall n > 4$ we have $\sqrt{n} < \frac{n}{2}$, and therefore b_j lies in $(-\frac{n}{2}, \frac{n}{2})$
The claim holds.

By Claim 2.1 and Claim 2.2 we get that $\hat{d} = f(m \cdot R^T) = m \cdot R^T$
Right multiplying by R we have,
$\hat{d} \cdot R = m \cdot R^T \cdot R = m \cdot R \cdot R^T = m \cdot I_n = m$
Therefore, $\boxed{\text{m} = \hat{d} \cdot R}$
Decryption works perfectly!

Cryptosystem Security

We know the ciphertext vector c which is given by c = $v \cdot \hat{L}$ + m .
Let $u = v \cdot \hat{L}$ be a vector. Since $v \in \mathbb{Z}^n$ this implies that u is vector that exists in integer lattice generated by $\hat{L}$. Therefore c is sum of a lattice vector u and our message m. Therefore this is a close vector problem looking for the vector closest to c such that we can subtract it from c to arrive at m.
Let $b_1, b_2, b_3, b_4.....b_n$ be orthogonal basis vectors of $\hat{L}$. We can express c in terms of these basis vectors (b_i) as :

$$c = \alpha_1 b_1 + \alpha_2 b_2 + ...\alpha_n b_n$$

We can find coefficients α_i by computing inner dot product $<$c,$b_i$$>$ as:

$$< c, b_i >= \begin{bmatrix} c_1 & c_2 & ..\, c_n \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ . \\ .b_n \end{bmatrix}$$

and dividing the product by length of vector b_i. Since $c, b_i \in \mathcal{Q}^N \implies \alpha_i \in \mathcal{Q}^N$.

We can use Babai's rounding technique to compute vector (let's say w) closest to our target vector c which exists in lattice generated by $\hat{L}$. In rounding technique we simply approximate coefficients α_i to their nearest integers and by taking modulo n to give w as:

$$w = \lfloor \alpha_1 \rceil\, b_1 + \lfloor \alpha_2 \rceil\, b_2 + ... + \lfloor \alpha_n \rceil\, b_n$$

After computing closest vector w we can get our plaintext message m by subtracting this closest vector w from our ciphertext vector c.

$$m = c - w$$

$$m = c - \lfloor \alpha_1 \rceil\, b_1 + \lfloor \alpha_2 \rceil\, b_2 + ... + \lfloor \alpha_n \rceil\, b_n$$

Yes there are other ways to break the security.

1. We can use LLL algorithm to get reduced basis from out input basis matrix $\hat{L}$. Then as explained in previous part we can use Babai's rounding technique to compute vector (let's say w) closest to our target vector c which exists in lattice generated by $\hat{L}$ and eventually can recover our message m.

2. As explained in previous part of the question breaking this cryptosystem is a CVP problem. We can use Babai nearest plane algorithm to solve Closest vector problem with our ciphertext vector c as a target vector and with basis vectors(b_i) of $\hat{L}$. The basic idea behind algorithm is:

We consider a plane (vector space) generated by (n - 1) lattice vectors. Then we find the translated plane at each lattice point and choose the one which is nearest to the target vector c. Apply the procedure inductively to the sublattice created by those n-1 vectors as well as to the new translated target vector. After computing closest vector(let's say v) using this algorithm we can get our message m by following way:

$$m = c - v$$

References

1. CS641A Lecture Slides by Dr. Manindra Agrawal
2. $https://cseweb.ucsd.edu/classes/wi12/cse206A-a/lec1.pdf$
3. $https://www.isical.ac.in/\ shashank_r/lattice.pdf$
4. $http://math.stmarys-ca.edu/wp-content/uploads/2017/07/Ahsan-Zahid.pdf$