[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Rathva Kaushikkumar Sanjaybhai (202051156)

Winter 2022-2023
Week : 2 (3nd lecture #)

1 Hill Cipher

It's an cipher which has a nxn matrix as a key.

$a_{ij} \in Z_{26}$

$A = (a_{ij})_{n \times n}$

where , *A is Secretkey and has to be invertible.*

$M = \{m_1\ m_2 \ldots m_n\} \leftarrow {Z_{26}}^n$ *possiblestrings.*

Here, M is plain text.

1.1 Encryption :

Cipher text $C = A \cdot M = (c_1\ c_2 \ldots c_n)$

1.2 Decryption :

Decrypted text $M = A^{-1} \cdot C$

2 Substitution Box

$S : \{A, B, \ldots Z\} \rightarrow \{A, B, \ldots, Z\}$

substitution box is Mapping on it self.
Where , $P \rightarrow C = S(P)$

Here everything is known just Mapping/Sbox is kept secret.

If, Mapping is bijective their can be 26! such mapppings.
But if it's not then their are 26^{26} mappings.

Secret key of the Sbox can be found out using brute force/Exhaustive search.