Lec 1 ~~Vist~~ Visit homepage ~ RITUMONI

Recap: • $\mathbb{Z}_n = \underbrace{\{0, 1, 2, \dots, n-1\}}$ $1 \to [1]$

Which is a ring $[a] + [b] = [a+b]$

$[a] = \{x \in \mathbb{Z} : n \mid x-a\}$

$a \in \mathbb{Z}$,

$a +_n b$ is the remainder when $a+b$ is divided by n.

$[a] \times [b] = [ab]$

$-[12] = ?$ if $n = 27$ $[0] = [27] = [54] \dots$

$[15]$

$[a]^{-1}$ make sense if $\exists$ $[b]$ s.t. $[a] \times [b] = [1]$

$\Longleftrightarrow$ $[a]^{-1}$ exists if & only if $\gcd(a, n) = 1$

$n = 26$, $[3]^{-1} = [9]$

Find $[3]^{-1}$ if $n = 27$?

does not exist.

$[4]^{-1} =$ for $n = 27$.

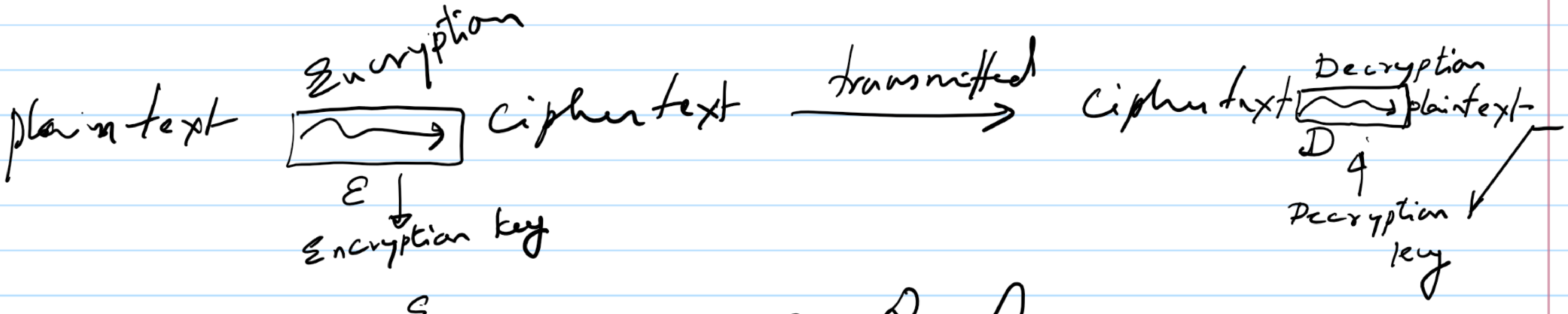
Cryptography: Secure communication.

- Confidentiality: privacy or secrecy
- Data integrity: to know if there is any change in data.
- Authentication: identification of originator of the message/data

Also it may have time of creation.

- Non-repudiation: Cannot refuse a previous commitment.

- Plain text: message to be transmitted
- Ciphertext: plain text is converted into a diff't form which is actually transmitted ~~to~~ which is called ciphertext.



$$\mathcal{P} \xrightarrow{\mathcal{E}} C \qquad C \xrightarrow{\mathcal{D}} \mathcal{P}$$

$$\mathcal{D} \circ \mathcal{E} = id_{\mathcal{P}} \qquad \mathcal{E} \circ \mathcal{D} = id_{C}$$

$\mathcal{E}$ & $\mathcal{D}$ are bijection (inverse of each other)

Word = a string of characters.

characters are letters from the alphabet $\{A, \dots, Z\}$ & —, ·, comma, ? and more perhaps

Encryption key is a word (or a value) which is used to encrypt a plain text to form the ciphertext.

Decryption key is ________________

Cryptanalysis: It is the study of deciphering ciphertext without the knowledge of decryption key.

Numerical equivalent of characters:

Monographs: Each single character is encrypted individually

Numerical equivalent

A	B	C	D	. . .	Z	—	dot	?
0	1	2	3	. . .	25	26	27	28

Here $n = 29$

Digraph:

A	B	C	D	Z	–	dot	?
00	01	02	03	25	26	27	28

- $N(OR) = N(O)N(R) = \underline{1315}$

- Using base: fix a base, say m

$$N(OR) = m \times N(O) + N(R)$$

Classical cipher: ∘ Substitution

shift $\quad \mathcal{E} : \mathcal{P} \longrightarrow \mathcal{C}$

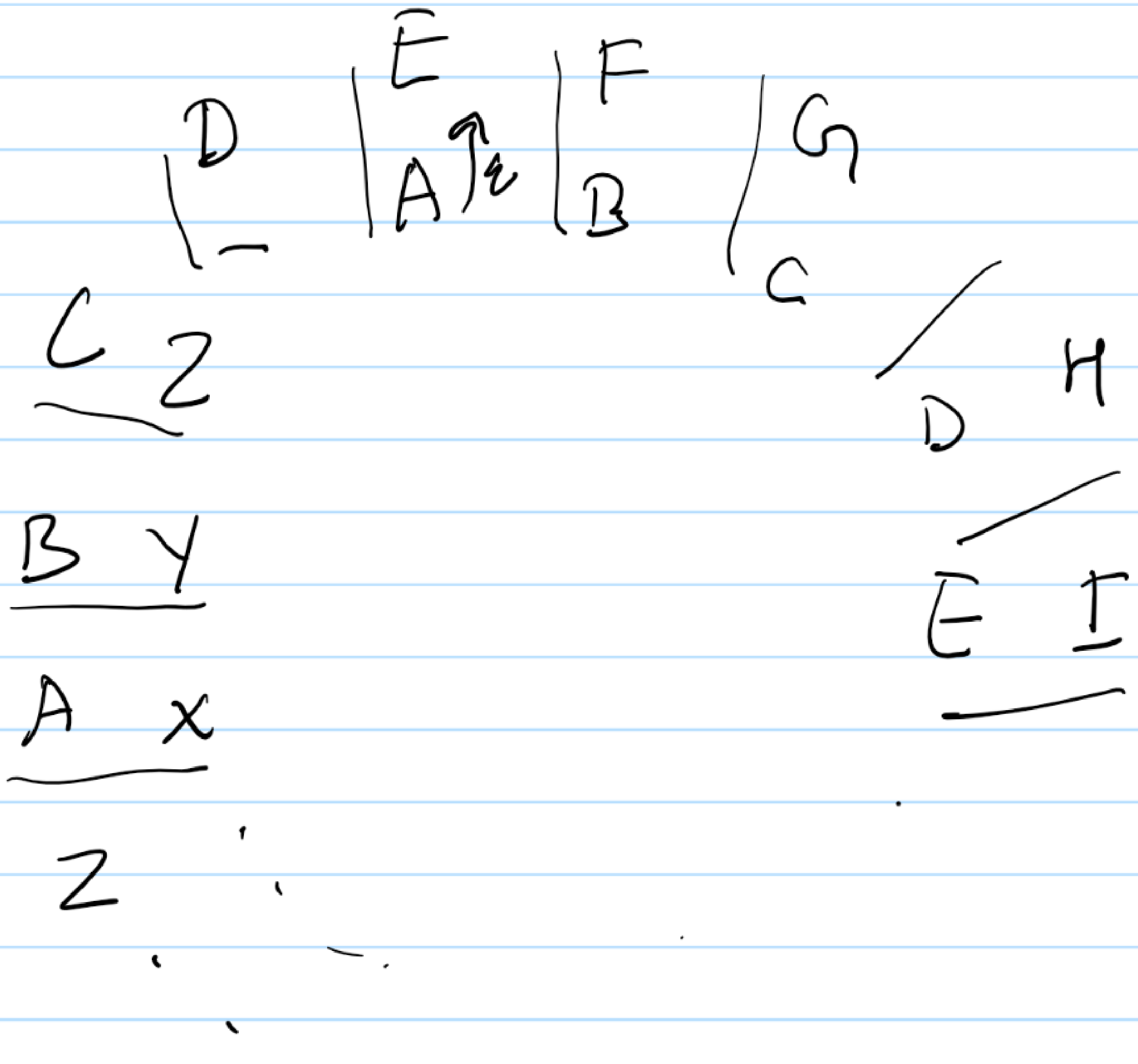
$$\mathcal{E}(x) = x + b \pmod{n} \qquad \text{if} \quad |\mathcal{A}| = n$$

$b = 4, \quad n = 27 \quad \mathcal{A} = \{A, B, \dots, Z, -\}$

$$\mathcal{E}(PASSWORD) = \mathcal{E}(P)\mathcal{E}(A)\mathcal{E}(S)\mathcal{E}(S) \cdots \mathcal{E}(D)$$

$$= TE \;\dots\; - \; - \; H$$

$$\begin{tikzcd} P \arrow[r, "N"] & \bigcirc \arrow[r, "\overset{\mathcal{E}}{+b}"] & \bigcirc \arrow[r, "N^{-1}"] & T \end{tikzcd}$$



$\mathcal{D} : \mathcal{C} \longrightarrow \mathcal{P}$

Decryption $D(x) = x - b$ (mod n)

Hill cipher:

$$\mathcal{E}(x) = kx \pmod{n}$$

since we want $\mathcal{E}$ to be a bijection $\underline{\gcd(k, n) = 1}$

$\mathcal{E}(ONE) = \underline{B-I}$ $n = 27$, $k = 2$

$N(O) = 14$, $\rightsquigarrow 2 \times 14 = 28$ mod 27)
$= 1$ (mod 27) $\overset{2}{\rightsquigarrow} B$

$N(N) = \underline{13} \rightsquigarrow 2 \times 13 = 26 = \rightsquigarrow -$

$N(E) = 4 \rightsquigarrow 2 \times 4 = 8 \rightsquigarrow I$

Decryption $D(x) = k^{-1}x$

For $n = 27$, $k = 2$, $2^{-1} = 14$ (mod 27)

$D(B-I) = ONE.$

$N(B) = 1 \rightsquigarrow 1 \times 14 \rightsquigarrow O$

$N(-) = 26 \rightsquigarrow 26 \times 14 = 13$ (mod 27) $\rightsquigarrow N$

$((-1) \times 14 = -14 = 27 - 14 = 13)$

$N(I) = 8 \longrightarrow 8 \times 14 = 4 \times 28 \equiv 4$ mod 27. $\rightarrow E$.

Affine cipher.

$\mathcal{E}(x) = kx + b$ where $\gcd(k, n) = 1$

$\underline{|A| = n}$ & $0 \leq b \leq n-1$

$D(x) = \underline{k^{-1}x - k^{-1}b}$

$\left[ky + b = x \Rightarrow ky = x - b \Rightarrow y = k^{-1}x - k^{-1}b \right]$