Semester : VI Subject : CSS Academic Year: 2023-2024

## Autokey Cipher :-

* The key in the autokey cipher is a stream of subkeys, each of which is used to encrypt the plaintext character it corresponds to.
* The first subkey is a secretly agreed-upon value among the communicating parties. The value of the first plaintext character is the second subkey.
* The value of the second plaintext character is the third subkey, and so on.
* Given plaintext $P = P_1 P_2 P_3 \ldots$ and key $K = (K_1, P_1, P_2 \ldots)$

Encryption : $C_i = (P_i + K_i) \bmod 26$

Decryption : $P_i = (C_i - K_i) \bmod 26$

Example:-

Encrypt the message "ATTACK IS TODAY" using autokey cipher with key = 12. Ignore the space between words.

Solution :

Encryption : $C_i = (P_i + K_j) \bmod 26$

| Plain Text | A | T | T | A | C | K | I | S | T | O | D | A | Y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ps Values | 00 | 19 | 19 | 00 | 02 | 10 | 08 | 18 | 19 | 14 | 03 | 00 | 24 |
| Key stream | 12 | 00 | 19 | 19 | 00 | 02 | 10 | 08 | 18 | 19 | 14 | 03 | 00 |
| Cs value | 12 | 19 | 12 | 19 | 02 | 12 | 18 | 00 | 11 | 07 | 17 | 03 | 24 |
| Cipher Text | M | T | M | T | C | M | S | A | L | H | R | D | Y |

The result is "MTMTCMSALHRDY".