

Tutorial-VII (Symmetric Ciphers & Revision)

1. (i) Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).
(ii) Use the affine cipher to decrypt the message “ZEBBW” with the key pair (7, 2) in modulus 26

2. Using the Rabin cryptosystem with $p = 47$ and $q = 11$:
(i) Encrypt $P = 17$ to find the ciphertext.
(ii) Use the Chinese remainder theorem to find four possible plaintexts.

3. In the elliptic curve $E(1, 2)$ over the $GF(11)$ field: (Revision Problem)
(i) Find all points on the curve and make a figure.
(ii) Generate public and private keys for Bob.
(iii) Choose a point on the curve as a plaintext for Alice.
(iv) Create ciphertext corresponding to the plaintext in part d for Alice.
(v) Decrypt the ciphertext for Bob to find the plaintext sent by Alice.