CRYPTOGRAPHY AND NETWORK SECURITY

MINOR CLASS TEST-1

AIMAN SIDDIQUA. - 2K18/MC/008

RSA cryptosystem.

$p = 5$, $q = 11$.

$n = p \times q = 55$

$\phi(n) = (p-1)(q-1) = 4 \times 10 = 40$

$e = 3$

$d = e^{-1} \bmod 40 \equiv 3^{-1} \bmod 40 \equiv (-13) \bmod 40 \equiv 27$

q	r_1	r_2	t_1	t_1	t_2	t
13	40	3	1	0	1	-13
3	3	1	0	1	-13	40
	1	0		-13	40	

Plaintext $P = 9$

$C = 9^3 \bmod 55 \equiv 729 \bmod 55 = 14$

FERMATS THEOREM

To calculate 2^{1000} in group $Z_{13}, +_{13}$

By fermat's little theorem

$$2^{12} \equiv 1 \bmod 13$$

$$2^{1000} \equiv 2^{400} \equiv 2^{40} \equiv 2^4 \equiv 16 \equiv 3 \bmod 13.$$

ELLIPTIC CURVE.

$$y^2 = x^3 + x + 6$$

$$d = 7 \quad e_1 = (2, 7)$$

$$P = (10, 9)$$

$$r = 3$$