MANIPAL UNIVERSITY JAIPUR

School of Information Technology

Department of Information Technology

Subject: Cryptography & Information Security [IT 3203]

Assignment 1

Q.1: Solve the following:

a) What is the multiplicative inverse of 10 mod 11? Solve it using extended Euclidean algorithm.

b) Check the validity of the statement: $10 \equiv 3 \bmod 12$.

c) Solve with the hill cipher. Plain text: “POH” Key: GYBNQKURP.

d) Decrypt the message “ymnsp dtz hfs” using the Caesar cipher with key=5.

e) Encipher the message “notification” Using rail fence cipher of column 3.

f) Encrypt the message “discovery” using the Vigenere cipher with key “google”.

g) Construct a Playfair matrix with the key “security”. Using the matrix encrypt the message “this is a secret key”.

Q.2: Explain RSA Algorithm. Perform encryption and decryption using RSA algorithms for prime numbers p=3, q=11, e=3 and message = 011101011.

Q.3: In a Diffie- Hellman key exchange algorithm, let the prime number be 11 and find its primitive root and let A and B select their secret key. XA=97 and XB=233. Compute the public key of A and B and common secret key.

Q.4: Draw the general structure of DES and explain the encryption-decryption process.

Q.5: Differentiate-

a) Hash code and message authentication code (MAC).

b) Key generation in AES and DES.

c) Mono and Poly alphabetic Ciphers.

Q.6: Find the prime factors p and q of n = 3233, given that n is the product of two prime numbers, and use them to calculate the private key exponent d, for the RSA algorithm, when the public key exponent e is 17.

Q.7: Consider a Diffie-Hellman key exchange between Alice and Bob. They agree to use a prime modulus p = 41 and base value g = 7. Alice chooses a secret number a = 10, while Bob chooses a secret number b = 20 then calculates the shared secret key.

Q.8: Given two prime numbers p = 17 and q = 11, calculate their product n and Euler's totient function φ(n). Choose an integer e=7 that is coprime to φ(n) and calculate its multiplicative inverse modulo φ(n).

Q.9: Utilize the extended Euclidean algorithm to find the greatest common divisor of 391 and 299, along with the coefficients x and y that satisfy the equation,

$$391+299=\gcd(391,299)391x+299y=\gcd(391,299).$$

Q.10: Apply the extended Euclidean algorithm to find integers x and y such that $7+26=17x+26y=1$

Q.11: In AES encryption if 128-bit key is W0 = 2b7e1516 W1 = 28aed2a6 W2 = abf71588 W3 =09cf4f3c determine the first-round key (W4 W5 W6 W7) if Constant for first round is 01 and consider standard AES S-Box.

Q.12: What is the output of Substitution-box process of DES encryption for the input block “101111” using standard S-BOX-1.