Assignment 31 Oct - Cryptography Solutions (With Explanations)

1. Diffie-Hellman Key Exchange

Parameters: p = 47, g = 2, A's private a = 7, B's private b = 11.

Step-by-step:

1) Compute A's public key: A = g^a mod p = 2^7 mod 47 = 2^7 = 128; 128 mod 47 = 34.

2) Compute B's public key: B = g^b mod p = 2^11 = 2048; 2048 mod 47 = 27.

3) Shared secret (A computes): s = B^a mod p = 27^{7} mod 47 => 21.
   (B would compute s = A^b mod p and get the same value.)

Result: A's public key = 34, B's public key = 27, Shared secret = 21.

2. RSA Encryption (p=11, q=17)

Parameters: p = 11, q = 17.

1) Compute n = p*q = 11*17 = 187.

2) Compute ϕ(n) = (p-1)(q-1) = 10*16 = 160.

3) Choose public exponent e such that 1 < e < ϕ(n) and gcd(e, ϕ(n)) = 1.
   We choose e = 7; gcd(7, 160) = 1.

4) Compute private exponent d as modular inverse of e modulo ϕ(n):
   Find d such that e*d ≡ 1 (mod 160). The inverse of 7 mod 160 is 23 because 7*23 = 161 ≡ 1 (mod 160).

Public key: (n, e) = (187, 7)

Private key: (n, d) = (187, 23)

Encryption of plaintext P = 9: C = P^e mod n = 9^7 mod 187 = 70.

Decryption: C^d mod n = 70^23 mod 187 = 9 (retrieves original plaintext).

3. Vigenère Cipher (Key = PEAR)

Plaintext (spaces removed): MEETMEATDAWN
Key (repeated): PEARPEARPEAR

Encryption steps (letter -> numeric -> add -> result):
Plain 'M' (12) + Key 'P' (15) -> B (1)
Plain 'E' (4) + Key 'E' (4) -> I (8)
Plain 'E' (4) + Key 'A' (0) -> E (4)
Plain 'T' (19) + Key 'R' (17) -> K (10)
Plain 'M' (12) + Key 'P' (15) -> B (1)
Plain 'E' (4) + Key 'E' (4) -> I (8)
Plain 'A' (0) + Key 'A' (0) -> A (0)
Plain 'T' (19) + Key 'R' (17) -> K (10)
Plain 'D' (3) + Key 'P' (15) -> S (18)
Plain 'A' (0) + Key 'E' (4) -> E (4)
Plain 'W' (22) + Key 'A' (0) -> W (22)
Plain 'N' (13) + Key 'R' (17) -> E (4)

Encrypted ciphertext: BIEKBIAKSEWE

4. Columnar Transposition Cipher (Key = PEAR)

Plaintext (spaces removed): MEETMEATDAWN
Key: PEAR -> column count = 4, rows = 3

Write plaintext row-wise into a grid:
  M E E T
  M E A T
  D A W N

Column read order (sorted letters of key): 'A'(index 2), 'E'(index 1), 'P'(index 0), 'R'(index 3)

Columns read in that order produce: