Q1. (a) In the RSA algorithm, why must we choose "e" to be relatively prime to Φ(n)? What happens if we break the rule gcd(e, Φ(n)) = 1 and choose an enciphering index e such that that gcd(e, Φ(n)) > 1? Justify your answer with the example M (message) = 2, p = 3, q = 5, e = 2 and n = pq. [Φ(n) is Euler Totient Function]

(b) Suppose an eavesdropper Eve knows N = pq and also Φ(n). Show that Eve can then find p and q.

(c) In the RSA algorithm show that the encryption key "e" must be odd. [4+3+3]

Q2. (a) Prove the following complementation properties of DES

$DES_{k'}(x') = (DES_k(x))'$ for any x and k

Here, x' denotes the bitwise complement of x, i.e. the bit string obtained by flipping all bits of x.

(b) Let B be a byte in bit form and let B' be B + 11111111, the complement of B. For fixed given key k, if AES encrypts B to G, does AES encrypt B' to G'? [6+4]

Q3. (a) Suppose the round keys for round 7 of AES is

A0 B1 C2 D3 E4 F5 6A 7B 8C 9D AF E9 D8 C7 B6 A5

What are the first 4 bytes of the round key for round 8 if 8th round constant is 80. Use AES S-Box for byte substitution.

(b) In the Forward Substitute Byte of AES, after computing the multiplicative inverse, byte transformation is performed by using the following function

$b_i' = b_i + b_{(i+4)mod8} + b_{(i+5)mod8} + b_{(i+6)mod8} + b_{(i+7)mod8} + c_i$

Here, B ($b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1\, b_0$) is the input byte and b_i' is the i-th bit of the output transformed byte B' and c_i is the i-th bit of the constant byte C. + represent the XOR operation.

Similarly, in the Inverse Substitute Byte of AES, the inverse byte transformation uses a constant byte D.

(i) Find the relation between the forward constant byte C and the inverse constant byte D

(ii) Find D when C = A1 [5+(2+3)]

Q4. Assume that someone sends the encrypted messages by using DES in the Output Feedback (OFB) mode of operation with a secret (but fixed) IV value

(a) Show how to perform the known-plaintext attack in order to decrypt the transmitted messages

(b) Is it better with the Cipher Feedback (CFB) mode?

(c) What about the Cipher Block Chaining (CBC) mode? [4+4+2]