Midterm: Part I

Note

This is a closed-book exam. Part I contains five problems, each accounting for 10 points.

Problems

1. (a) Why in DES the round function need not be invertible?
   (b) What does it mean to say that DES has a good avalanche effect?
2. Consider the AES algorithm, where the irreducible polynomial modulus is $x^8+x^4+x^3+x+1$.
   (a) What is the result of (1101 1001) $\cdot$ (0000 0101)? Show the steps of your calculation.
   (b) What is the value of $(0111\ 1011)^{-1}$? Show the steps of your calculation.
3. What are modes of operation for block ciphers? Why are they needed? Please name four of them.
4. Describe by example centralized and decentralized key distributions. How do they compare?
5. Consider the following communication protocol: each node N in the network has been assigned a unique secret key K_n. This key is used to secure communication between the node and a trusted server, which stores all the keys. User A, wishing to send a secret message M to user B, initiates the following protocol:
   (a) A generates a random number R and sends to the server (1) his name A, (2) destination B, and (3) $E(K_a, R)$.
   (b) The server responds by sending $E(K_b, R)$ to A.
   (c) A sends $E(R, M)$ together with $E(K_b, R)$ to B.
   (d) B knows K_b, thus decrypts $E(K_b, R)$ to get R and will subsequently use R to decrypt $E(R, M)$ to get M.

   An intruder with legal access to one of the network nodes may be able to obtain the plain text of any secret message that has been transmitted between two other nodes. Please describe such an attack.

Appendix

- The extended Euclid's algorithm for polynomials is as follows.

EXTENDED EUCLID$(m(x), b(x))$:

1. $[A_1(x), A_2(x), A_3(x)] \leftarrow [1, 0, m(x)]; [B_1(x), B_2(x), B_3(x)] \leftarrow [0, 1, b(x)]$
2. if $B_3(x) = 0$ then return $A_3(x) = \gcd(m(x), b(x))$; no inverse
3. if $B_3(x) = 1$ then return $A_3(x) = \gcd(m(x), b(x)); B_2(x) = b^{-1}(x) \pmod{m(x)}$
4. $Q(x) =$ the quotient of $A_3(x)/B_3(x)$
5. $[T_1(x), T_2(x), T_3(x)] \leftarrow [A_1(x) - Q(x)B_1(x), A_2(x) - Q(x)B_2(x), A_3(x) - Q(x)B_3(x)]$
6. $[A_1(x), A_2(x), A_3(x)] \leftarrow [B_1(x), B_2(x), B_3(x)]$
7. $[B_1(x), B_2(x), B_3(x)] \leftarrow [T_1(x), T_2(x), T_3(x)]$
8. goto 2