Midterm: Part I

Note

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

Problems

1. A permutation operation on n (≥ 1) distinct objects (arranged in some order so that each object is uniquely identifiable by a number in $\{1, 2, \cdots, n\}$) can be represented by a table listing a permutation of the numbers from $\{1, 2, \cdots, n\}$ in the following sense: if the i-th entry of the table is p_i, then the new i-th object will be the original p_i-th object. For example, the following P is a permutation operation on 8 objects:

$$P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 5 & 3 & 2 & 6 & 7 & 1 \end{bmatrix}$$

   Given the input $M = \langle M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8 \rangle$, P produces the output $P(M) = \langle M_4, M_8, M_5, M_3, M_2, M_6, M_7, M_1 \rangle$.

   (a) Give the inverse permutation P^{-1} of the above P using the same representation.

   (b) Let $[r_1 r_2 \cdots r_{n-1} r_n]$ be the inverse of a given permutation $[p_1 p_2 \cdots p_{n-1} p_n]$. Describe in precise mathematical terms the relation between r_i's and p_i's.

2. (a) Why in DES the round function (**F**) need not be invertible?

   (b) How does three-key triple DES achieve backward compatibility with DES? Please describe all alternatives.

3. 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 0110) $\cdot$ (0000 1010)? Show the steps of your calculation.

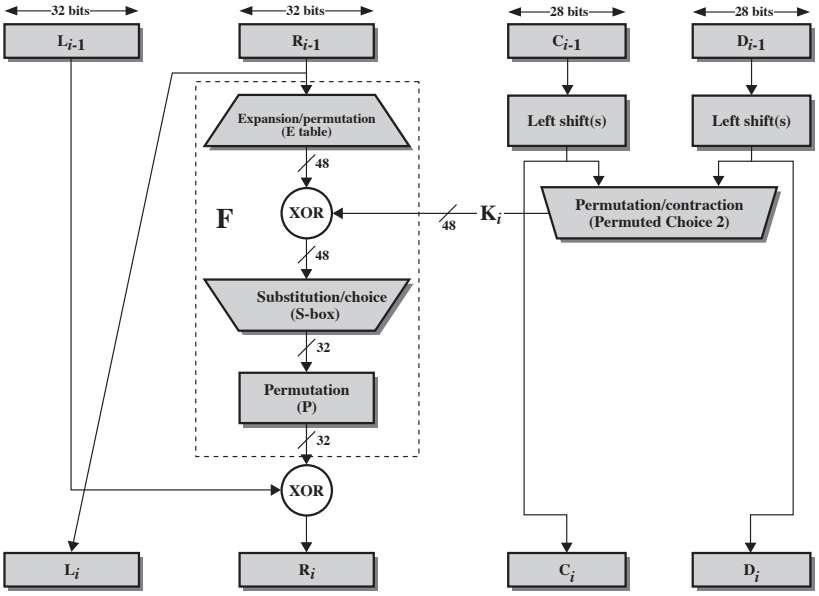
   (b) What is the value of $(1010\ 0101)^{-1}$? Show the steps of your calculation.

4. Consider pseudorandom number generation with the OFB mode of operation using 128-bit encryption. Suppose, as an observer (not knowing the seed value), you have observed so far n *different* blocks $C_1, C_2, \ldots, C_n$ of pseudorandom bits on the output. What is the probability that the stream of blocks will start to repeat itself from the next block? Please justify your answer. Make assumptions that you think are necessary.

5. Describe by example centralized and decentralized key distributions. How do they compare?

Appendix

- Single round of DES Algorithm:



- Extended Euclid's algorithm for polynomials:

$EXTENDED\ EUCLID(a(x), b(x))$:

1. $[V_1(x), W_1(x), R_1(x)] \leftarrow [1, 0, a(x)]; [V_2(x), W_2(x), R_2(x)] \leftarrow [0, 1, b(x)]$
2. if $R_2(x) = 0$ then return $R_1(x) = \gcd(a(x), b(x))$; no inverse
3. if $R_2(x) = 1$ then return $R_2(x) = \gcd(a(x), b(x)); W_2(x) = b^{-1}(x) \pmod{a(x)}$
4. $Q(x) =$ the quotient of $R_1(x)/R_2(x)$
5. $[V(x), W(x), R(x)]$
   $\leftarrow [V_1(x) - Q(x)V_2(x), W_1(x) - Q(x)W_2(x), R_1(x) - Q(x)R_2(x)]$
6. $[V_1(x), W_1(x), R_1(x)] \leftarrow [V_2(x), W_2(x), R_2(x)]$
7. $[V_2(x), W_2(x), R_2(x)] \leftarrow [V(x), W(x), R(x)]$
8. goto 2

- Pseudorandom number generation with the OFB mode: