Midterm: Part I

Note

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

Problems

1. (a) What does it mean to say that DES has a good avalanche effect?
   (b) How does three-key triple DES achieve backward compatibility with DES? Please describe all alternatives.

2. This problem concerns finite fields of the form GF(2^3).
   (a) To construct a GF(2^3), one needs to choose an irreducible polynomial of degree 3 as the modulus. Is $x^3 + 1$ irreducible? Please justify your answer.
   (b) Suppose we choose $x^3 + x^2 + 1$ as the irreducible polynomial. Please use the generator approach to produce a table of multiplication for the GF(2^3) defined by $x^3 + x^2 + 1$.

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 (0101 1011) $\cdot$ (0000 0110)? Show the steps of your calculation.
   (b) What is the value of $(0110\ 0011)^{-1}$? Show the steps of your calculation.

4. Using AES, decryption takes a slightly longer time than encryption.
   (a) Which operation and its inverse are most responsible for this difference? Why does the inverse takes a longer time than the original operation?
   (b) Why is this difference not reflected in the encryption and decryption with some modes of operation?

5. How can an encryption algorithm be used for pseudorandom number generation? Please describe a scheme. Assuming that the 256-bit AES is used, what is the period of the generated bit stream?

Appendix

- 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

- AES encryption and decryption: