Midterm: Part I

Note

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

Problems

1. Consider the AES algorithm, where the irreducible polynomial modulus is $x^8+x^4+x^3+x+1$.

   (a) What is the result of (1110 1011) $\cdot$ (0000 0101)? Show the steps of your calculation.

   (b) What is the value of $(0101\ 1101)^{-1}$? Show the steps of your calculation.

2. 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?

3. If a bit error occurs in the transmission of a ciphertext character in the Cipher Feedback (CFB) Mode of Operation, how far does the error propagate? Please explain.

4. A variant of the Linear Congruential Method for pseudorandom number generation applies the following equation to iteratively generate a sequence of numbers.

   $$X_{n+1} = (aX_n) \bmod m$$

   where m ($m > 0$) is the modulus, a ($0 \leq a < m$) is the multiplier, and X_0 ($0 \leq X_0 < m$) is the starting value (seed).

   (a) What is the longest possible period attainable with this scheme? Why?

   (b) How should the parameters be set up to guarantee the longest possible period? Please try to be as general as possible.

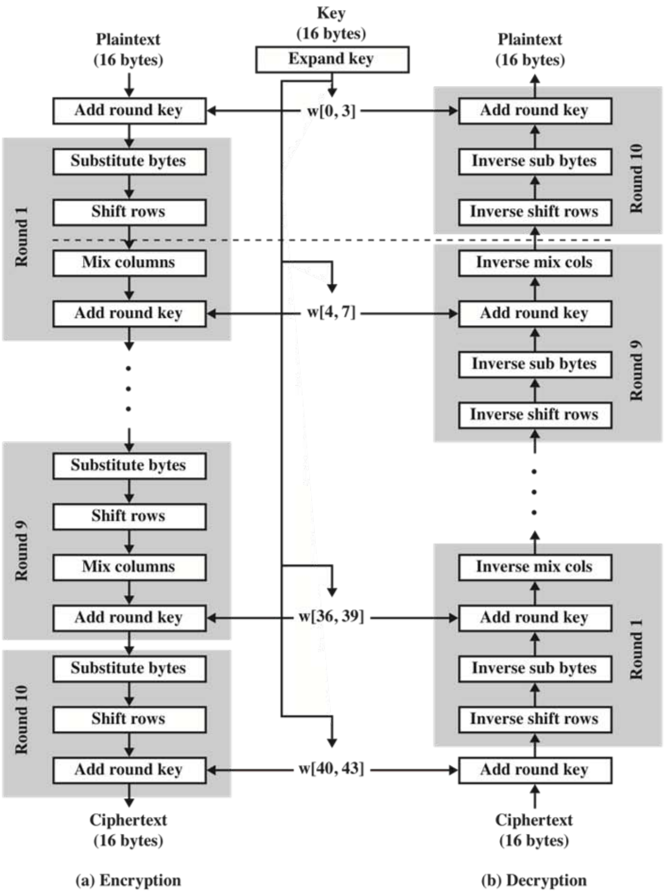
5. How can an encryption algorithm be used for pseudorandom number generation? Please describe a scheme. Assuming that an encryption algorithm with a 128-bit block size is used, what is the period of the generated bit stream? (Note: the unit of length here is one bit.)

Appendix

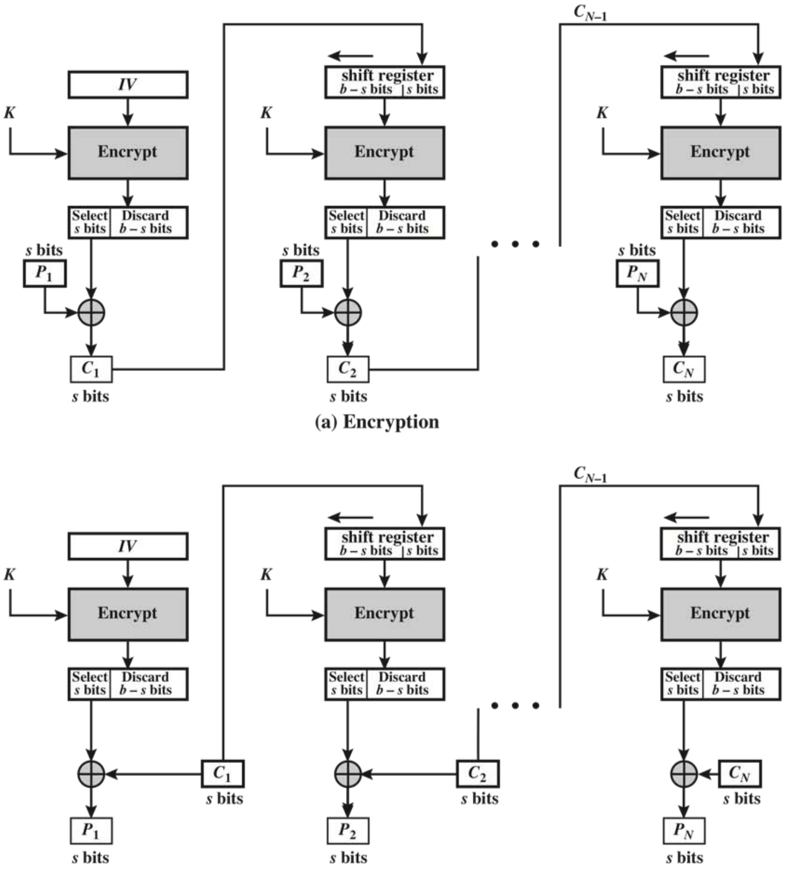
- Extended Euclid's algorithm for polynomials:

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



- The Cipher Feedback (CFB) Mode of Operation:



(a) Encryption

(b) Decryption