Midterm: Part I

Note

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

Problems

1. Consider known-plaintext attacks on the 3×3 Hill cipher. What are the criteria on the known plaintext-ciphertext pairs for an attack to succeed? Please be as precise as possible and explain the reasons for such criteria.

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 (0110 1101) $\cdot$ (0000 0110)? Show the steps of your calculation.

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

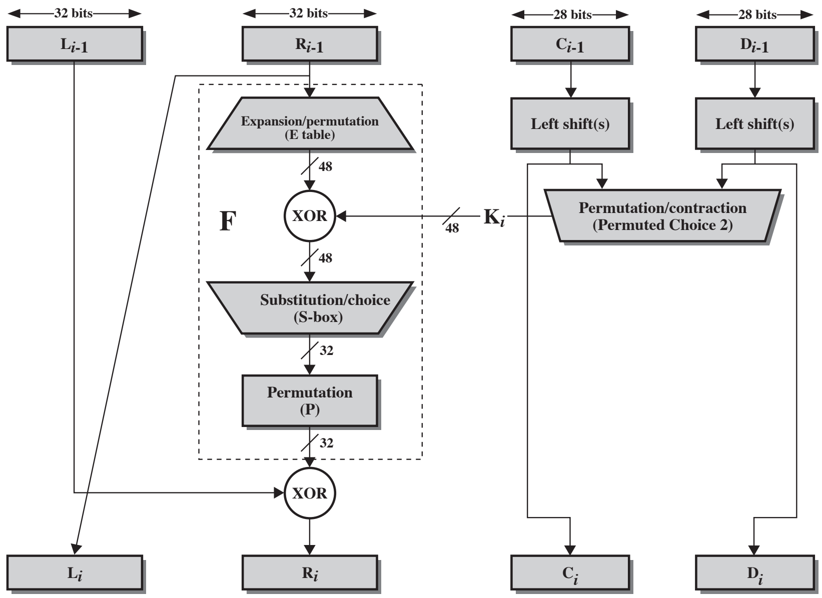
   (a) If the next block C_{n+1} would be equal to any of the previous blocks, it must be C_1. Why?

   (b) What is the probability that the stream of blocks will start to repeat itself from C_{n+1}?

   Please justify your answers.

Appendix

- Single round of the DES Algorithm:

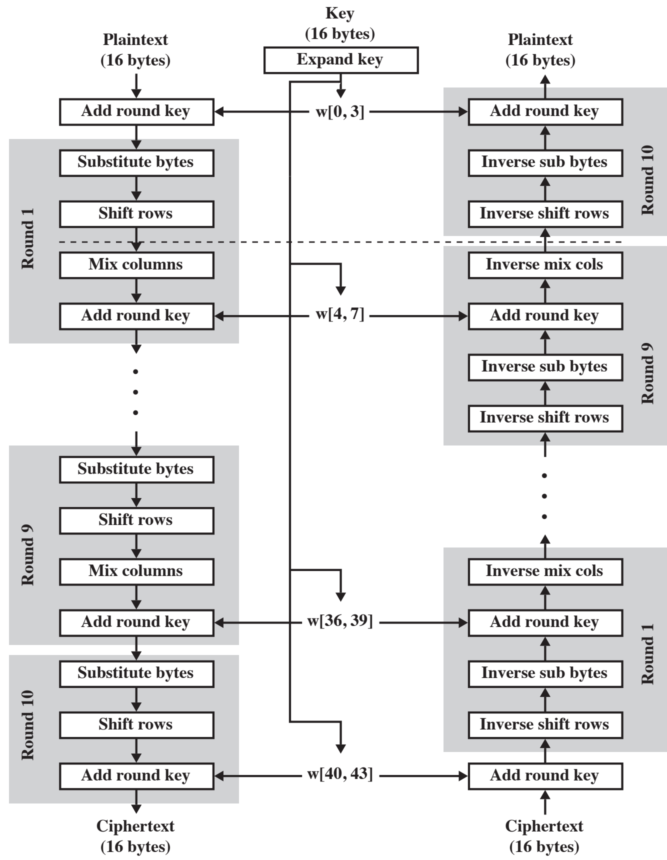


- Extended Euclid's algorithm for polynomials:

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

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

- AES encryption and decryption:



(a) Encryption (b) Decryption

- Pseudorandom number generation with the OFB mode: