

Midterm: Part I

Note

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

Problems

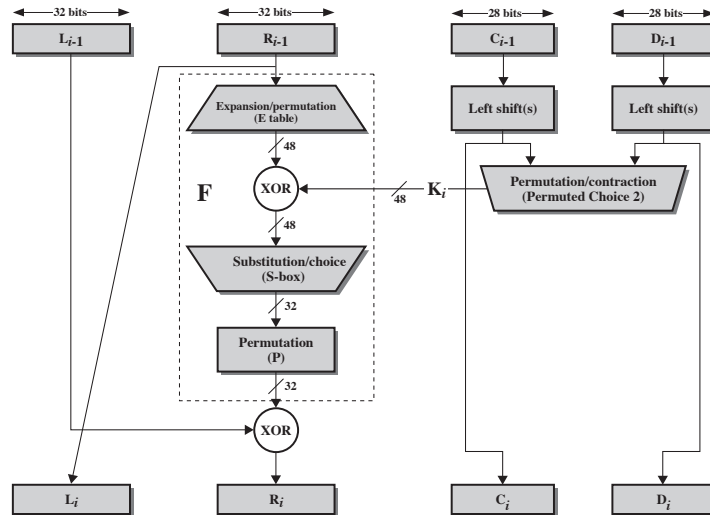
1. Answer the following questions concerning DES.
 - (a) Why in DES the round function (\mathbf{F}) need not be invertible?
 - (b) What does it mean to say that DES has a good avalanche effect?
2. Consider the AES algorithm, where the irreducible polynomial modulus is $x^8 + x^4 + x^3 + x + 1$.
 - (a) What is the result of $(0110\ 1101) \cdot (0000\ 0111)$? Show the steps of your calculation.
 - (b) What is the value of $(0110\ 1110)^{-1}$? Show the steps of your calculation.
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?
4. Answer the following questions concerning the Counter (CTR) Mode of Operation for block ciphers.
 - (a) (6 points) What are the main advantages of the CTR mode? Please give three of them.
 - (b) (4 points) Does the CTR mode have any weakness? Please explain.
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, \dots, 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:

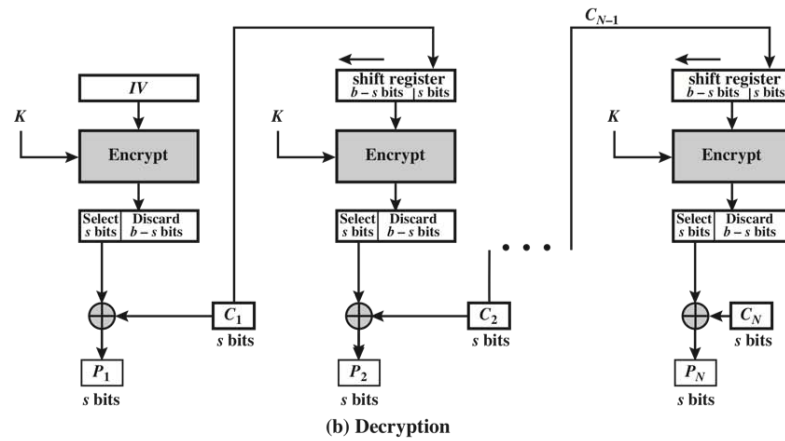
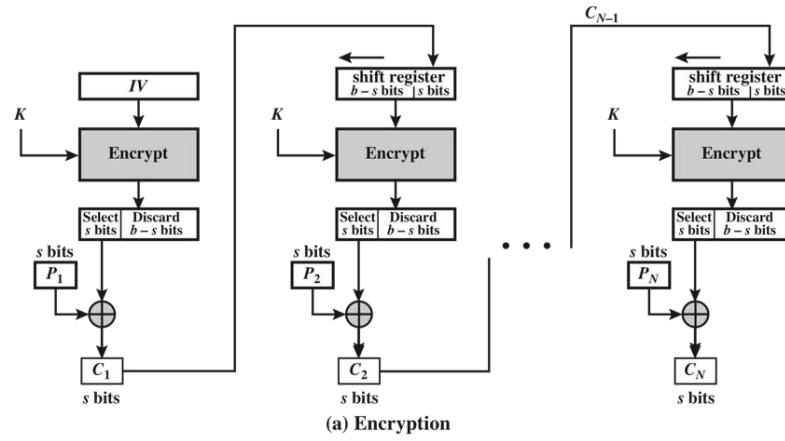


- Extended Euclid's algorithm for polynomials:

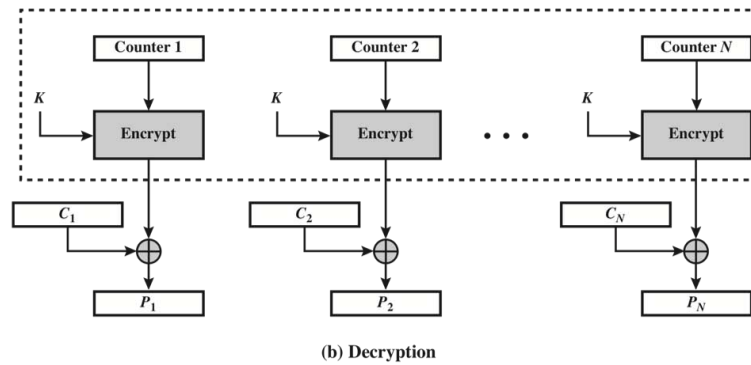
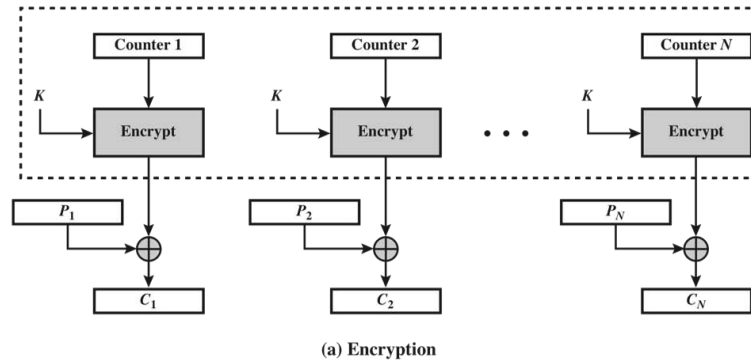
EXTENDED EUCLID($a(x), b(x)$) :

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

- The Cipher Feedback (CFB) Mode of Operation:



- The Counter (CTR) Mode of Operation:



- Pseudorandom number generation with the OFB mode:

