Cryptography　　　Midterm Exam　　　2010/04/27

Part I　(3 points each)

1. Which irreducible polynomial over GF_5 is *primitive*?
   A. x^2+2　B. x^2+x+1　C. x^2+2x+3　D. x^2+4x+1　E. None of the above

2. Which multiplicative group is NOT of order 36?
   A. $\mathbf{Z}_{37}$*　B. $\mathbf{Z}_{63}$*　C. $\mathbf{Z}_{108}$*　D. $\mathbf{Z}_{126}$*　E. None of the above

3. $\alpha \in GF_8$ is a root of x^3+x^2+1. Whose minimal polynomial is x^3+x+1?
   A. α^2　B. α^4　C. $\alpha^4+\alpha^2$　D. $\alpha^4+\alpha^3$　E. None of the above

4. Which is NOT a finalist of the AES selection?
   A. Mars　B. Rijndael　C. Twofish　D. IDEA　E. None of the above

5. For a group homomorphism f: ($\mathbf{Z}_{16}$, + mod 16) → ($\mathbf{Z}_{17}$*, × mod 17), which assignment of the value of $f(1)$ makes f an *isomorphism*?
   A. 2　B. 4　C. 6　D. 8　E. None of the above

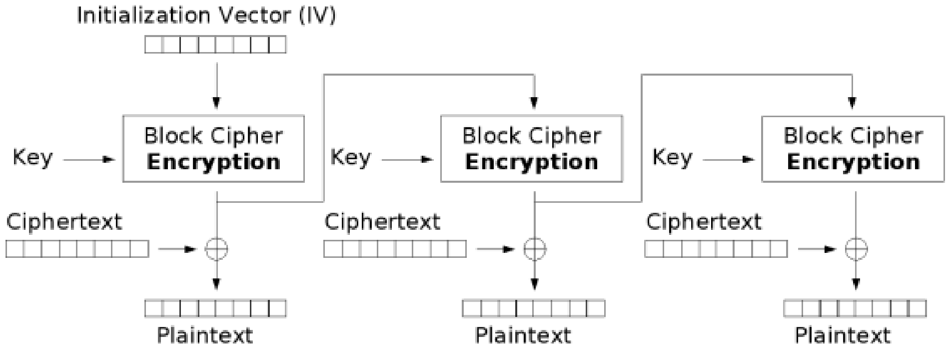
6. Which ideal is NOT a *principal* ideal in the specified ring?
   A. $<x, y>$ in $\mathbf{Z}[x, y]$　B. $<x^2-1>$ in $Q[x, y]$
   C. $<6, 15, 33>$ in Z　D. $<x+1, x^2>$ in $Q[x]$　E. None of the above

7. Which quotient ring is isomorphic to GF_{64}?
   A. $GF_2[x]/<x^6+x^5+x^4+x^3+x^2+x+1>$　B. $GF_2[x]/<x^6+x^4+x^3+x^2+1>$
   C. $GF_2[x]/<x^6+x^2+1>$　D. $GF_2[x]/<x^6+x^4+x^3+1>$　E. None of the above

8. In the "Mix Columns" operation of AES, each column is treated as a polynomial over GF_{256} and is multiplied modulo $r(x)$ with fixed $3x^3+x^2+x+2$. What is $r(x)$?
   A. x^4　B. x^4+1　C. x^4+x+1　D. x^4+x^2+1　E. None of the above

9. Which statement about the *one-time pad* (OTP) is FALSE?
   A. XOR operation is often used to combine the plaintext and the key elements
   B. It is *information-theoretically secure* with the so-called *perfect secrecy*
   C. To be unbreakable, its key has to be truly random and never reused
   D. Such system with the *perfect secrecy* property is widely used in practice
   E. None of the above

10. Which mode of operation for decryption does the diagram below show?
A. OFB B. CFB C. ECB. D.CBC E. None of the above



Part II (3 points each)

- $x \equiv$ [11] (mod [12]) is the solution to the system of congruences
  $2x \equiv 1 \pmod 3$ $\quad x \equiv 3 \pmod{10}$ $\quad 5x \equiv 4 \pmod{67}$

- To prove that x is a generator of the multiplicative group Z_{63}^*, it is sufficient to show $x^m \neq 1$ and $x^n \neq 1$ where $0 < m < n$. We have $(m, n) =$ ([13], [14]).

- $GL_3(Z_7)$ is the group of invertible 3×3 matrices with entries in Z_7, and $SL_3(Z_7)$ is its subgroup consisting of the matrices with determinant 1. Their group orders are $|GL_3(Z_7)| =$ [15] and $|SL_3(Z_7)| =$ [16].

- In the multiplicative group $(\mathbf{Z}_{65}^*, \times)$:
  - 17^{-1} (the multiplicative inverse of 17) = [17].
  - $o(3)$ (the order of 3) = [18].

- Since $P(x) = x^5 + 2x + 2$ is irreducible over GF_3, the quotient ring $K = GF_3[x]/(P(x))$ is a finite field. Let $Q(x) = x^2 + 2x + 1$.
  - The number of elements in K is $|K| =$ [19].
  - $Q(x)^{1213} = 2x^3 +$ [20] in K.
  - $Q(x)^{-1} = x^4 +$ [21] in K.

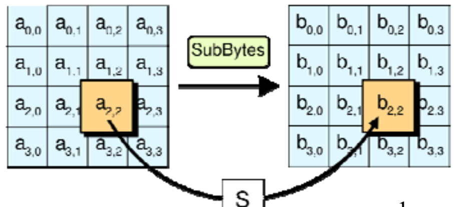
- Complete the table:

Block cipher	Block size (bits)	Key size (bits)
Triple-DES	64	112 or [22]
IDEA	64	128
AES	128	128, 192, or [23]
SMS4	[24]	128

- Applying the secret permutation $\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,4\,6\,2\,1\,5 \end{pmatrix} \in S_6$ on the plaintext CRYPTO, we obtain the ciphertext TPCROY. Suppose the permutation $\sigma \in S_6$ is applied on CRYPTO to obtain POCTYR, then $\sigma^2 = \boxed{25}$ and $\sigma^{-1} = \boxed{26}$.

- Consider the affine cipher $c = mp + s \mod 50$, where c and p denote the ciphertext and the plaintext respectively:
  - ♦ The size of its key space (possibilities of (m, s)) is $\boxed{27}$.
  - ♦ Given the encryption formula $c = 7p + 11 \mod 50$, the corresponding decryption formula is $p = \boxed{28} \mod 50$.

- The S-box of AES is constructed as follows.
  - ♦ $a_{i,j} \to a_{i,j}^{-1} \to b_{i,j}$
  - ♦ $a_{i,j} \times a_{i,j}^{-1} = 1 \pmod{x^8+x^4+x^3+x+1}$ but $0^{-1} = 0$
  - ♦ Affine transformation: $a_{i,j}^{-1} \to b_{i,j}$
  - ♦ Complete the last mapping:
    - ◦ $00000000 \to 00000000 \to 01100011$
    - ◦ $00000001 \to 00000001 \to 01111100$
    - ◦ $00000011 \to \boxed{29} \to \boxed{30}$

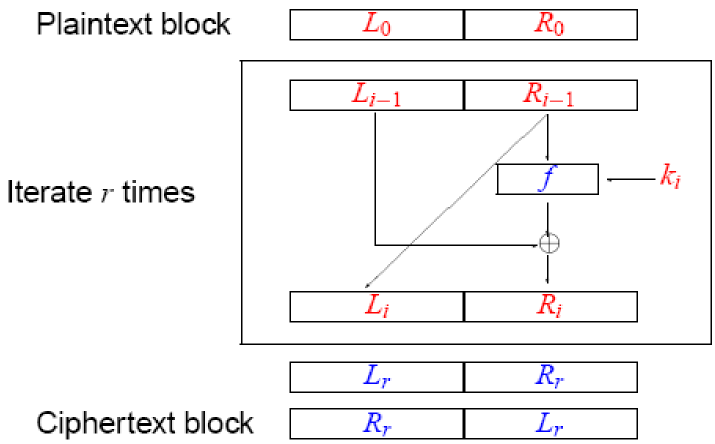


$$\underbrace{\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix}}_{b_{i,j}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}}_{a_{i,j}^{-1}} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Part III (Write down all details of your work)

$\boxed{31}$ (4 points) Find integers a and b such that $31a + 53b = 1$.

$\boxed{32}$ (6 points) Explain why a block cipher of Feistel structure has the same algorithm for both encryption and decryption.



Cryptography Midterm Exam 2010/04/27

Name: ____________ Student ID number: ____________

1	2	3	4	5	6	7	8	9	10

11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

31

32

Cryptography Midterm Exam 2010/04/27

Solution

1	2	3	4	5	6	7	8	9	10
C	E	C	D	C	A	E	B	D	A

11	12	13	14	15
443	2010	12	18	$(7^3-1)(7^3-7)(7^3-7^2)$
16	**17**	**18**	**19**	**20**
$7^2(7^3-1)(7^3-7)$	23	12	243	x^2+x+1
21	**22**	**23**	**24**	**25**
$2x^3+2x^2+2$	168	256	128	(15)(34)
26	**27**	**28**	**29**	**30**
(1453)(26)	1000	$43(c-11)$	1111 0110	0111 1011

31 $a = 12$, $b = -7$

32