Cryptography Midterm Exam 2011/04/19

Part I (3 points each)

1. Which multiplicative group is isomorphic to $(\mathbf{Z}_5^*, \times)$?
   A. $(\mathbf{Z}_8^*, \times)$ B. $(\mathbf{Z}_{10}^*, \times)$ C. $(\mathbf{Z}_{12}^*, \times)$ D. $(\mathbf{Z}_{15}^*, \times)$ E. None of the above

2. Which can NOT be the number of elements of a Galois Field?
   A. 97 B. 64 C. 49 D. 36 E. None of the above

3. Which ideal is NOT the same as the principal ideal $<6>$ in Z?
   A. $<-6>$ B. $<18,-24>$ C. $<36,48>$ D. $<60,72,-30>$ E. None of the above

4. Which is a generator (primitive element) of the multiplicative group Z_{41}^*?
   A. 2 B. 3 C. 4 D. 5 E. None of the above

5. An S-box is denoted by "$m \times n$" if its inputs and outputs are m-bit and n-bit long respectively. How to denote the S-boxes of DES?
   A. 8×8 B. 4×4 C. 8×6 D. 6×4 E. None of the above

6. Which quotient ring is isomorphic to GF_{125}?
   A. $GF_5[x]/<x^3+2x+1>$ B. $GF_5[x]/<x^3+x^2+3>$
   C. $GF_5[x]/<x^3+2x+2>$ D. $GF_5[x]/<x^3+x^2+4>$ E. None of the above

7. Which is the best description of the Caesar Cipher?
   A. Hill Cipher B. Substitution Cipher
   C. Shift Cipher D. Permutation Cipher E. None of the above

8. Without which operation, AES becomes a cipher operating on four independent 32-bit blocks, that is, 1-bit change in plaintext affects 32-bit range in ciphertext?
   A. ByteSub B. ShiftRow
   C. MixColumn D. KeyAddition E. None of the above

9. Which statement is true for AES?
   A. The S-box for ByteSub operation is also used in the key schedule
   B. Designed by Joan Daemen and Vincent Rijmen of IBM, USA
   C. Constructed as the structure of Feistel cipher
   D. Some operations are performed in the Galois Field GF_{128}
   E. None of the above

10. Which statement is true for block cipher modes of operation?
   A. ECB needs initialization vectors (IV)
   B. CBC ciphertext depends on all previous blocks
   C. OFB keystream is generated by encrypting ciphertext
   D. CFB has no ciphertext error propagation
   E. None of the above

Part II (3 points each)

- $a =$ $\boxed{11}$ and $b =$ $\boxed{12}$ is the pair of integers satisfying $61a + 43b = 1$ with the condition that *a* is the least positive one.

- In the multiplicative group $(\mathbf{Z}_{61}{}^*, \times)$:
  - ♦ 43^{-1} (the multiplicative inverse of 43) = $\boxed{13}$.
  - ♦ $o(9)$ (the order of 9) = $\boxed{14}$.
  - ♦ To prove that 2 is a generator of the group, it is sufficient to show that $2^u \neq 1$, $2^v \neq 1$, and $2^w \neq 1$. If $1 < u < v < w < 61$, then $v =$ $\boxed{15}$ and $w =$ $\boxed{16}$.

- $x \equiv$ $\boxed{17}$ (mod $\boxed{18}$) is the solution to the equation $396x \equiv 308 \pmod{968}$

- A subset H of a group $(G, *)$ is a subgroup of G if and only if
  - ♦ $\boxed{19}$ $\in H$ for all $a, b \in H$; and
  - ♦ $\boxed{20}$ $\in H$ for all $a \in H$.

- Galois field GF_{64} is unique up to isomorphism.
  - ♦ GF_{64} consists of all roots of $f(x) =$ $\boxed{21}$ of degree 64 over GF_2.
  - ♦ Represent GF_{64} by the quotient ring $K = GF_2[x] / < x^6 + x^5 + x^3 + g(x) >$, then $g(x) =$ $\boxed{22}$ of degree 2 over GF_2.
  - ♦ $h(x)$ is a polynomial of degree ≤ 5 over GF_2 satisfying the relation of cosets $[x^{2011}] = [h(x)]$ in *K*, then $h(x) =$ $\boxed{23}$. [Hint: Reducing the exponent to an integer (could be negative) with a small absolute value might reduce the computation significantly]

- Clarify the potential of parallel processing for the following modes of operation:
  (A) ECB (B) CBC (C) OFB (D) CFB
  The cipher operations can be performed in parallel if the input block to each cipher does not depend on the result of the previous cipher operation.
  - ♦ In the encryption of $\boxed{24}$, ciphers can be computed in parallel if plaintext blocks are immediately available.
  - ♦ In the decryption of $\boxed{25}$, ciphers can be computed in parallel if ciphertext blocks are immediately available.
    [Note: Fill in A, B, C, or D. There might be two or more to fill in one blank.]

- Complete the table:

Block cipher	DES	AES		
Block size (bits)	**26**	128		
Key size (bits)	56	**27**	192	256
Number of rounds	16	**28**	12	14

- The S-box of AES is constructed as follows.
  - $a_{i,j} \rightarrow a_{i,j}^{-1} \rightarrow b_{i,j}$
  - $a_{i,j} \times a_{i,j}^{-1} = 1 \pmod{x^8+x^4+x^3+x+1}$ but $0^{-1} = 0$
  - Affine transformation: $a_{i,j}^{-1} \rightarrow b_{i,j}$
  - Complete the last mapping in hexadecimal:
    - 00 $\longrightarrow$ 00 $\longrightarrow$ 63 [= $(01100011)_2$]
    - 01 $\longrightarrow$ 01 $\longrightarrow$ 7C [= $(01111100)_2$]
    - 0F $\longrightarrow$ $\boxed{29}$ $\longrightarrow$ $\boxed{30}$

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

Part III (Write down all details of your work)

$\boxed{31}$ (3 points) Prove that the inverse of any element g in a group G is unique.

$\boxed{32}$ (3 points) To show that the Galois field GF_8 is unique up to isomorphism, construct an isomorphism between the quotient rings

$$R_1 = GF_2[x]/<x^3+x^2+1> \quad \text{and} \quad R_2 = GF_2[x]/<x^3+x+1>.$$

That is, determine $h(x) \in GF_2[x]$ such that the homomorphism $f: R_1 \rightarrow R_2$ defined by $f([0]) = [0]$, $f([1]) = [1]$, and $f([x]) = [h(x)]$ is one-to-one and onto, where $[t]$ denotes the coset that t belongs to. Explain why your choice is correct.

$\boxed{33}$ (4 points) Every input column $\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$ and output column $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$ of the MixColumn operation of AES is treated as $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ and $b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$ over GF_{256} respectively. A fixed polynomial $c(x) = c_3x^3 + c_2x^2 + c_1x + c_0$ is selected in advance to perform the MixColumn transformation $b(x) = a(x)c(x) \bmod (x^4+1)$ over GF_{256}. Derive the assignments of b_i's in terms of a_i's and c_i's in matrix form. That is, find a 4×4 matrix M such that $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = M \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$.

Cryptography　　Midterm Exam　　2011/04/19

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 ~ 33

Cryptography Midterm Exam 2011/04/19

Solution

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

11	12	13	14	15
12	-17	44	5	20
16	**17**	**18**	**19**	**20**
30	13	22	$a * b$	a^{-1}
21	**22**	**23**	**24**	**25**
$x^{64} - x$	$x^2 + 1$	$x^5 + x + 1$	A	ABD
26	**27**	**28**	**29**	**30**
64	128	10	C7	76

31

32 $h(x) = x + 1$, $x^2 + x + 1$, or $x^2 + 1$

33