Cryptography Midterm Exam I 2008/04/07

Part I (3 points each)

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

2. Which is a generator of the multiplicative group GF_{13}*?
   A. 4 B. 5 C. 8 D. 9 E. None of the above

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

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

5. In a Feistel cipher, every encryption round consists of $L_i = R_{i-1}$ and
   A. $R_i = R_{i-1} \oplus f(L_{i-1}, k_i)$ B. $R_i = R_{i-1} \oplus f(R_{i-1}, k_i)$
   C. $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$ D. $R_i = L_{i-1} \oplus f(L_{i-1}, k_i)$
   E. None of the above

6. Which is NOT a finalist of the AES selection?
   A. Serpent B. Twofish
   C. Rijndael D. RC4 E. None of the above

7. $GF_2[x]/(x^8+x^4+x^3+x+1)$ is selected to represent $GF(2^8)$ in AES. In hexadecimal expressions, which is the multiplicative inverse of '3A' represented by $x^5+x^4+x^3+x$?
   A. '0E' B. '16' C. '20' D. '3B' E. None of the above

8. In many implementations of AES, decryptions are faster than encryptions. It is mainly caused by which operation?
   A. MixColumn B. AddRoundKey
   C. ShiftRow D. SubByte E. None of the above

9. Which can NOT replace the square matrix in the affine transformation constructing the S-box of AES to become a new block cipher?

A. $\begin{bmatrix} 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \end{bmatrix}$ B. $\begin{bmatrix} 1&1&0&1&0&1&1&0 \\ 0&1&1&0&1&0&1&1 \\ 1&0&1&1&0&1&0&1 \\ 1&1&0&1&1&0&1&0 \\ 0&1&1&0&1&1&0&1 \\ 1&0&1&1&0&1&1&0 \\ 0&1&0&1&1&0&1&1 \\ 1&0&1&0&1&1&0&1 \end{bmatrix}$ C. $\begin{bmatrix} 1&0&0&0&1&0&0&1 \\ 1&1&0&0&0&1&0&0 \\ 0&1&1&0&0&0&1&0 \\ 0&0&1&1&0&0&0&1 \\ 1&0&0&1&1&0&0&0 \\ 0&1&0&0&1&1&0&0 \\ 0&0&1&0&0&1&1&0 \\ 0&0&0&1&0&0&1&1 \end{bmatrix}$ D. $\begin{bmatrix} 1&0&0&0&1&1&1&0 \\ 0&1&0&0&0&1&1&1 \\ 1&0&1&0&0&0&1&1 \\ 1&1&0&1&0&0&0&1 \\ 1&1&1&0&1&0&0&0 \\ 0&1&1&1&0&1&0&0 \\ 0&0&1&1&1&0&1&0 \\ 0&0&0&1&1&1&0&1 \end{bmatrix}$

E. None of the above

10. Which statement is FALSE about the *self-synchronizing* stream cipher?
A. The keystream is independent of the ciphertext string
B. The remaining decryption fails if the synchronization is lost
C. Encryption in small quantities, such as bit or byte
D. No protection against message manipulation
E. None of the above

Part II (3 points each)

- In the multiplicative group $(\boldsymbol{Z}_{35}^*, \times)$:
  - 24^{-1} (the multiplicative inverse of 24) = $\boxed{11}$.
  - $|\boldsymbol{Z}_{35}^*|$ (the order of the group) = $\boxed{12}$.
  - $o(3)$ (the order of 3) = $\boxed{13}$.

- In the symmetric group S_6:
  - $|S_6| = \boxed{14}$.
  - $(16425)^{-1} = \boxed{15}$.
  - $(15364)(253)(14) = \boxed{16}$.

    ["Left-to-right" product here. For example, (123)(24) = (1423).]

- Consider the affine cipher $c = mp + s \mod 40$, where c and p denote the ciphertext and the plaintext respectively:
  - The size of its key space (possibilities of (m, s)) is $\boxed{17}$.
  - Given the encryption formula $c = 3p + 16 \mod 40$, the corresponding decryption formula is $p = \boxed{18}$ mod 40.

- The solution to the congruence equation $75x \equiv 10 \pmod{505}$ is $x \equiv \boxed{19} \pmod{\boxed{20}}$.

- To prove that α is a generator of the multiplicative group GF_{625}*, it is sufficient to show that $\alpha^a \neq 1$, $\alpha^b \neq 1$, and $\alpha^c \neq 1$. If $1 < a < b < c < 625$, then $a =$ [21] and $c =$ [22].

- Consider the sequence generated by an LFSR of linear complexity 4: 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, …
  - The corresponding connection polynomial is [23].
  - The period of the sequence is [24].
  - The next **three** bits ($11^{th} \sim 13^{th}$ bit) of the sequence are [25].

- $GL_2(GF_5)$ = The group of invertible 2×2 matrices with entries in GF_5.
  - $|GL_2(GF_5)|$ (the order of the group) = [26].
  - $|SL_2(GF_5)|$ (the order of the subgroup with determinant 1) = [27].

- Fill in the data block size of DES and AES, and the number of different S-boxes of DES:

	DES	AES		
Key Size (bits)	56	128	192	256
Block Size (bits)	[28]	[29]		
Number of Rounds	16	10	12	14
Number of Different S-box(s)	[30]	1		

Part III (Write down all details of your work)

[31] (4 points) Introduce one of the eSTREAM phase 3 candidates, which should be the same one on your homework.

- Write down the name of the stream cipher.
- Sketch its algorithm, analysis, performance, etc.

[32] (3 points) Find integers a and b such that $28a + 37b = 1$.

[33] (3 points) Over GF_2, find polynomials $f(x)$ and $g(x)$ such that
$$f(x)(x^2 + x) + g(x)(x^4 + x + 1) = \gcd(x^2 + x,\ x^4 + x + 1).$$

Cryptography Midterm Exam I 2008/04/07

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	33

Cryptography　　Midterm Exam I　　2008/04/07

Solution

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

11	12	13	14	15
19	24	12	720	(15246)
16	**17**	**18**	**19**	**20**
(25)(136)	640	$27(C-16)$	54	101
21	**22**	**23**	**24**	**25**
48	312	x^4+x+1	15	0,0,0
26	**27**	**28**	**29**	**30**
480	120	64	128	8

$\boxed{32}$ $a = 4, b = 3$

$\boxed{33}$ $f = x^4 + x + 1,\ g = 1$