Cryptography Midterm Exam 2013/04/16

Part I (3 points each)

1. Which quotient ring is NOT isomorphic to GF_{32}?
A. $GF_2[x] / < x^5+x^4+x^3+x+1 >$ B. $GF_2[x] / < x^5+x^3+1 >$
C. $GF_2[x] / < x^5+x^4+x^3+x^2+1 >$ D. $GF_2[x] / < x^5+x^4+1 >$ E. None of the above

2. Which irreducible polynomial over GF_3 is *primitive*?
A. x^3+2x+1 B. x^3+2x+2 C. x^3+x^2+2 D. x^3+x^2+x+2 E. None of the above

3. Which is the *effective key length* of three-key triple DES?
A. 84 B. 112 C. 128 D. 168 E. None of the above

4. Assume a company with 200 employees. A new security policy demands encrypted message exchange with a symmetric cipher. How many keys are required, if a secret communication is ensured for every possible pair of communicating parties?
A. 199 B. 200 C. 1990 D. 2000 E. None of the above

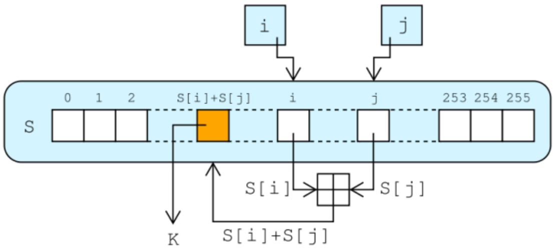
5. In a Feistel cipher, every encryption round consists of $L_i = R_{i-1}$ and
A. $R_i = L_{i-1} \oplus f(L_{i-1}, k_i)$ B. $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$
C. $R_i = R_{i-1} \oplus f(R_{i-1}, k_i)$ D. $R_i = R_{i-1} \oplus f(L_{i-1}, k_i)$ E. None of the above

6. The encryption of the block cipher IDEA mixes operations from three different algebraic groups. Which is NOT one of the groups?
A. $(\{0, 1\}^{16}, \oplus$ (XOR)) B. ($\mathbf{Z}_{65536}$, + mod 65536)
C. (S_{16}, $\circ$ (composition)) D. ($\mathbf{Z}_{65537}^*$, × mod 65537) E. None of the above

7. Let m_i's and c_i's be plaintext and ciphertext blocks respectively. With a decryption algorithm d and a key k, which is the decryption operation of CBC mode for $i > 1$?
A. $m_i = d_k(c_i) \oplus m_{i-1}$ B. $m_i = d_k(c_i \oplus m_{i-1})$
C. $m_i = d_k(c_i) \oplus c_{i-1}$ D. $m_i = d_k(c_i \oplus c_{i-1})$ E. None of the above

8. The block cipher SAFER (Secure And Fast Encryption Routine) has the 8-bit S-box constructed by $S(x) = 45^x \bmod 257$, where 256 is represented by 0. Apparently, $(\mathbf{Z}_{257}^*, \times) = <45>$, i.e., 45 is a generator (primitive root) of the cyclic group $\mathbf{Z}_{257}^*$. Which of the following mappings is NOT a bijective 8-bit S-box?
A. $S(x) = 45^{5x} \bmod 257$ B. $S(x) = 45^{6x} \bmod 257$
C. $S(x) = 45^{9x} \bmod 257$ D. $S(x) = 45^{15x} \bmod 257$ E. None of the above

9. Which stream cipher has the keystream generation shown by the figure, where one byte K is generated in each iteration?
A. RC4 B. SEAL C. Crypto1
D. A5/1 E. None of the above



10. Which statement is FALSE?
A. The key length of 128 bits is sufficient for long term (several decades) security even if practical quantum computers are present
B. Obtaining a secret key by measuring the electrical power consumption of a processor which operates on the secret key is an example of side-channel analysis
C. Kerckhoff's Principle means that a cryptosystem should be secure even if an attacker knows all details about the system, with the exception of the secret key
D. All encryption schemes from ancient times until 1976 were symmetric ones
E. None of the above

Part II (3 points each)

- Euler's Theorem and Fermat Little Theorem
    - $2^{2013}\cdot 3^{4}\cdot 5^{16} \bmod 13 = \boxed{11}$ (between 0 and 12)
    - $3^{2013}\cdot 5^{4}\cdot 9^{16} \bmod 14 = \boxed{12}$ (between 0 and 13)

  [If you saw the home page of Google yesterday, then you learned that yesterday (2013.4.15) was the 306th birthday of Leonhard Euler]

- Consider the multiplicative group $G = \boldsymbol{Z}_{31}{}^{*}$.
    - The order of 27 in G is $\boxed{13}$. [Note $27 \equiv -4 \pmod{31}$]
    - The solution to the discrete logarithm $3^{x} \equiv 22 \pmod{31}$ is $x = \boxed{14}$.

- The sequence 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, … is generated by an LFSR of degree 4.
    - The period of the sequence is $\boxed{15}$.
    - The next three bits (11th ~ 13th bit) of the sequence are $\boxed{16}$.

- A. ECB B. CBC C. OFB D. CFB E. CTR F. GCM
  From the above list of modes of operations, select appropriate ones satisfying the following specified property respectively.
    - Both the encryption and decryption functions of a block cipher are used: $\boxed{17}$
    - Decryption can be parallelized while encryption can NOT be parallelized: $\boxed{18}$
    - A one-bit transmission error of ciphertext affects only one bit of the decrypted plaintext: $\boxed{19}$

- $a =$ $\boxed{20}$ and $b =$ $\boxed{21}$ is the pair of integers satisfying $37a + 256b = 1$, where a is the *least positive* one. If an affine cipher has the encryption formula $y = 37x + 91 \bmod 256$, where $x, y \in \mathbf{Z}_{256}$ are plaintext and ciphertext respectively, then the decryption formula is $x =$ $\boxed{22}$ mod 256.

- Complete the table for DES and AES:

	DES	AES		
Key Length (bits)	56	128	192	256
Block Length (bits)	64	$\boxed{23}$		
Number of Rounds	$\boxed{24}$	10	12	$\boxed{25}$
Number of Different S-box(s)	$\boxed{26}$	1		

- Complete the table of key lengths of algorithms for different security levels:

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Symmetric-key	PRESENT, AES	80	128	192	256
Elliptic Curves	ECDH, ECDSA	160	256	$\boxed{27}$	512
Integer Factorization, Discrete Logarithm	RSA, DSA, ElGamal, DH (Diffie-Hellman)	1024	$\boxed{28}$	7680	15360

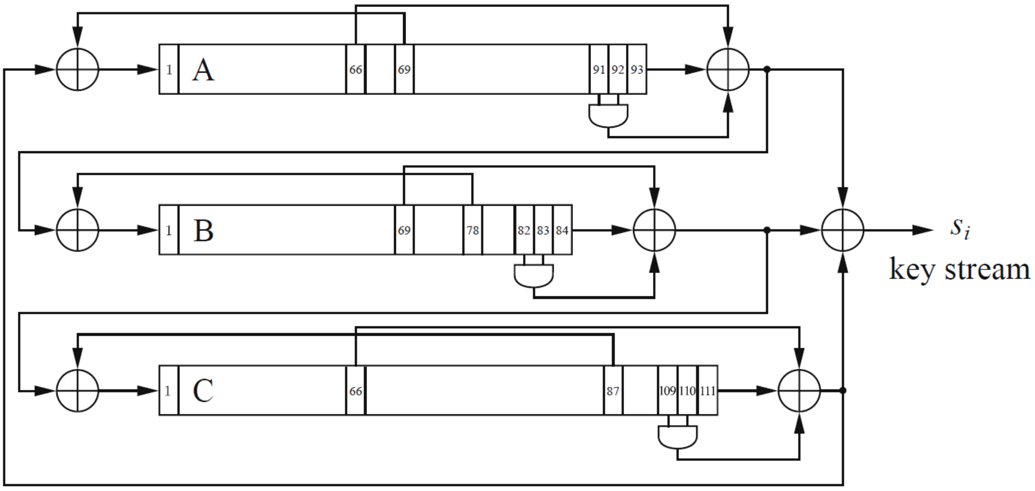
- Consider a simple brute force attack on DES which runs on COPACOBANA. Assume the implementation details as below.
    - COPACOBANA platform with 20 FPGA modules
    - 6 FPGAs per FPGA module
    - 4 DES engines per FPGA
    - Each DES engine is fully pipelined and is capable of performing one encryption per clock cycle
    - 100 MHz clock frequency

♦ The average runtime of an exhaustive key-search on DES is $\boxed{29}$ days (rounded to the closest integer).

♦ To achieve the average search time of one hour, $\boxed{30}$ COPACOBANA machines are required.

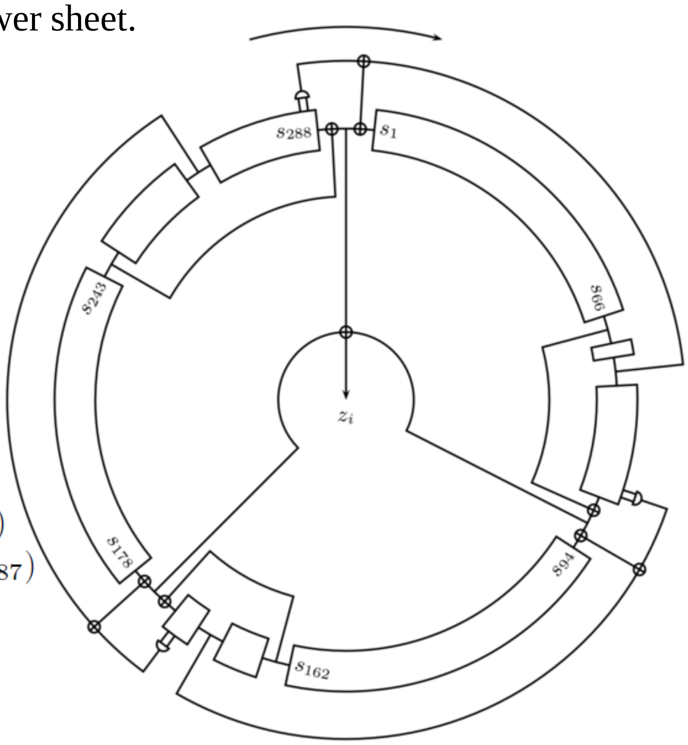
Part III (Write down all details of your work)

31 (3 points) The internal structure of the stream cipher Trivium is shown as the following diagram on the textbook. Unfortunately, this diagram is wrong.



The specification of the key stream generation of Trivium is as below. Draw the correct diagram on the answer sheet.

```
for $i = 1$ to $N$ do
    $t_1 \leftarrow s_{66} + s_{93}$
    $t_2 \leftarrow s_{162} + s_{177}$
    $t_3 \leftarrow s_{243} + s_{288}$
    $z_i \leftarrow t_1 + t_2 + t_3$
    $t_1 \leftarrow t_1 + s_{91} \cdot s_{92} + s_{171}$
    $t_2 \leftarrow t_2 + s_{175} \cdot s_{176} + s_{264}$
    $t_3 \leftarrow t_3 + s_{286} \cdot s_{287} + s_{69}$
    $(s_1, s_2, \ldots, s_{93}) \leftarrow (t_3, s_1, \ldots, s_{92})$
    $(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (t_1, s_{94}, \ldots, s_{176})$
    $(s_{178}, s_{279}, \ldots, s_{288}) \leftarrow (t_2, s_{178}, \ldots, s_{287})$
end for
```



32 (7 points)

(i) Besides $P(x) = x^4+x+1$, list all irreducible polynomials of degree 4 over $GF(2)$.

(ii) Factor $x^{16}-x$ over $GF(2)$.

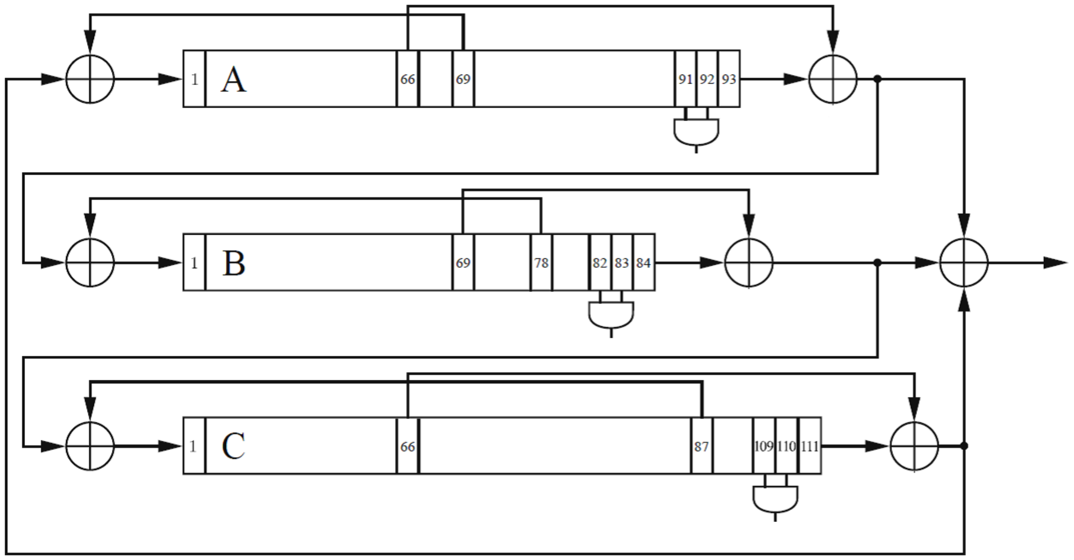
(iii) Compute $(x^3+x+1)/(x^2+x)$ in $GF(2^4)$ which is represented by $P(x)$.

Cryptography Midterm Exam 2013/04/16

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 2013/04/16

Solution

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr>
<tr><td>D</td><td>A</td><td>B</td><td>E</td><td>B</td><td>C</td><td>C</td><td>B</td><td>A</td><td>A</td></tr>
<tr><td colspan="2">11</td><td colspan="2">12</td><td colspan="2">13</td><td colspan="2">14</td><td colspan="2">15</td></tr>
<tr><td colspan="2">2</td><td colspan="2">3</td><td colspan="2">10</td><td colspan="2">17</td><td colspan="2">15</td></tr>
<tr><td colspan="2">16</td><td colspan="2">17</td><td colspan="2">18</td><td colspan="2">19</td><td colspan="2">20</td></tr>
<tr><td colspan="2">0, 0, 0</td><td colspan="2">AB</td><td colspan="2">BD</td><td colspan="2">CEF</td><td colspan="2">173</td></tr>
<tr><td colspan="2">21</td><td colspan="2">22</td><td colspan="2">23</td><td colspan="2">24</td><td colspan="2">25</td></tr>
<tr><td colspan="2">–25</td><td colspan="2">$173(y-91)$</td><td colspan="2">128</td><td colspan="2">16</td><td colspan="2">14</td></tr>
<tr><td colspan="2">26</td><td colspan="2">27</td><td colspan="2">28</td><td colspan="2">29</td><td colspan="2">30</td></tr>
<tr><td colspan="2">8</td><td colspan="2">384</td><td colspan="2">3072</td><td colspan="2">9 (≈8.696)</td><td colspan="2">209 (≈208.7)</td></tr>
</table>

31

32

(i) $x^4+x^3+1,\ x^4+x^3+x^2+x+1$

(ii) $x\,(x+1)\,(x^2+x+1)\,(x^4+x+1)\,(x^4+x^3+1)\,(x^4+x^3+x^2+x+1)$

(iii) x^2 $[(x^2+x)^{-1} = x^2+x+1]$