Cryptography Midterm Exam I 2007/04/16

Part I (3 points each)

1. Which value of Legendre symbol or Jacoby symbol is correct?

   A. $\left(\frac{13}{53}\right) = -1$ B. $\left(\frac{15}{55}\right) = -1$ C. $\left(\frac{17}{57}\right) = -1$

   D. $\left(\frac{19}{59}\right) = -1$ E. None of the above

2. Denote h as a hash function, k as a key, m as a message, p_1 and p_2 as padding strings. Which is the value of $HMAC_k(m)$?

   A. $h(k \| m)$ B. $h(m \| k)$ C. $h(k \| p \| m \| k)$

   D. $h(k \| p_1 \| h(k \| p_2 \| m))$ E. None of the above

3. Whose size of the key space is approximately equal to the complexity of finding a collision of SHA-224?

   A. 192-bit AES B. 256-bit AES C. 2-key Triple-DES

   D. 3-key Triple-DES E. None of the above

4. Which hash function is simply a truncated version of SHA-512, computed with different initial values?

   A. SHA-384 B. SHA-256 C. MD5

   D. RIPEMD-160 E. None of the above

5. In which operation of AES, each set of four bytes in a state is treated as a degree-3 polynomial over $\boldsymbol{F}_{256}$?

   A. ByteSub B. MixColumn C. AddRoundKey

   D. ShiftRow E. None of the above

6. By which mode of operation, a block cipher can be used to construct a *self-synchronizing* stream cipher?

   A. ECB B. CBC C. OFB D. CFB E. None of the above

7. Which value of Euler ϕ-function is NOT equal to 40?

   A. $\phi(41)$ B. $\phi(75)$ C. $\phi(88)$ D. $\phi(132)$ E. None of the above

8. In a Feistel cipher, every encryption round consists of $L_i = R_{i-1}$ and

A. $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$ B. $R_i = L_{i-1} \oplus f(L_{i-1}, k_i)$
C. $R_i = R_{i-1} \oplus f(L_{i-1}, k_i)$ D. $R_i = R_{i-1} \oplus f(R_{i-1}, k_i)$
E. None of the above

9. Which is true about the symmetric group S_5?

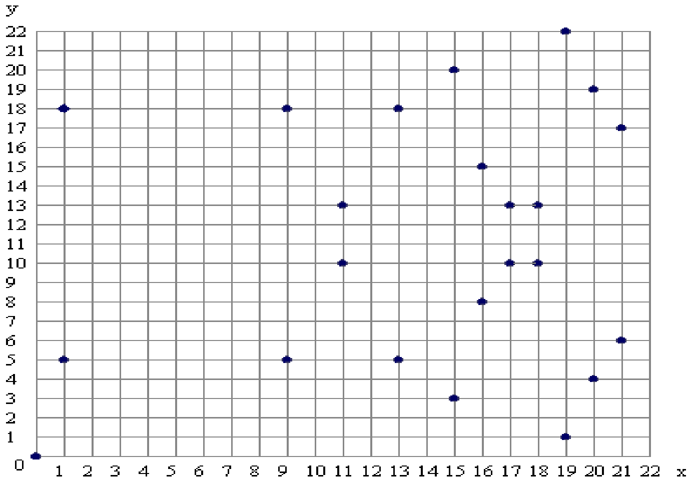
A. $|S_5| = 60$ B. $<(1, 2, 3, 4, 5)>$ is a normal subgroup
C. $(S_5 : S_4) = 10$ D. $(S_5 : <(1, 2, 3), (1, 2)>) = 30$
E. None of the above

10. Which statement is FALSE about the eSTREAM project?

A. The goal is to identify new stream ciphers that might become suitable for widespread adoption
B. Profile 1 contains submissions of stream ciphers for hardware applications with high throughput requirements
C. Profile 2 contains submissions of stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption
D. Profile 1A or 2A contains stream ciphers satisfying Profile 1 or 2 with an associated authentication method respectively
E. None of the above

Part II (3 points each)

- Consider the elliptic curve group defined by $y^2 = x^3 + x$ over $\boldsymbol{F}_{23}$. There are 23 points satisfying the equation as the graph below. Let $P = (1, 5)$ and $Q = (9, 18)$.
  - ■ The order of the elliptic curve group is $\boxed{11}$.
  - ■ $P + Q = \boxed{12}$.
  - ■ $-Q = \boxed{13}$.
  - ■ $2P = \boxed{14}$.
  - ■ $4P = \boxed{15}$.
  - ■ $2007P = \boxed{16}$.



- Since $P(x) = x^5 + 2x + 1$ is irreducible over $\boldsymbol{F}_3$, the quotient ring $K = \boldsymbol{F}_3[x]/(P(x))$ is a finite field. Let $Q(x) = x^2 + 2x + 1$.
  - ■ The number of elements in K is $|K| = \boxed{17}$.
  - ■ $Q(x)^{1213} = 2x^3 + \boxed{18}$ in K.
  - ■ $Q(x)^{-1} = x^4 + \boxed{19}$ in K.
  - ■ To prove that $P(x)$ is primitive, it is sufficient to show $x^m \neq 1$ and $x^n \neq 1$ in K where $m, n > 0$. We have $min(m, n) = \boxed{20}$.

- Consider the integer values of x satisfying

$$x \equiv 11 \pmod{27} \quad \text{and} \quad x \equiv 10 \pmod{29}.$$

  - ■ The smallest positive solution is $x = \boxed{21}$.
  - ■ The largest negative solution is $x = \boxed{22}$.

- For a set G, we denote $(G, +)$ as an additive group and $(G, \times)$ as a multiplicative group respectively. Consider the homomorphism

  $h: (\boldsymbol{Z}, +) \rightarrow (\boldsymbol{Z}_{31}{}^*, \times)$ defined by $h(x) = 4^x \bmod 31$.

  - ■ $(\boldsymbol{Z}/\mathrm{Ker}(h), +)$ is isomorphic to $(\boldsymbol{Z}_n, +)$ where $n = \boxed{23}$.
  - ■ The index $((\boldsymbol{Z}_{31}{}^*, \times) : (\mathrm{Im}(h), \times)) = \boxed{24}$.
  - ■ Apparently 4 is not a generator of the cyclic group $(\boldsymbol{Z}_{31}{}^*, \times)$. The smallest positive integer generating $(\boldsymbol{Z}_{31}{}^*, \times)$ is $\boxed{25}$.

- Assume the periodic sequence 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, … of period 7 is generated by an LFSR (Linear Feedback Shift Register).
  - ■ If the connection polynomial is primitive, it is $\boxed{26}$.
  - ■ The *linear complexity* of the sequence is $\boxed{27}$.

- Determine the period of the sequence generated by LFSR of register length 8 with non-zero initial state and connection polynomial $C(x)$.
  - ■ $C(x) = x^8 + x^5 + x^3 + x^2 + 1$ (primitive), then the period is $\boxed{28}$.
  - ■ $C(x) = x^8 + x^5 + x^4 + x^3 + 1$ (irreducible but not primitive), then the period is $\boxed{29}$. (Hint: Less than 30)
  - ■ $C(x) = x^8 + x^5 + x^3 + 1$ (reducible), then the maximal possible period is $\boxed{30}$.

Part III (Write down all details of your work)

$\boxed{31}$ (2 points)
Sketch the flow chart of CBC-MAC.

$\boxed{32}$ (3 points)
Sketch the flow chart of OFB mode (Output Feedback), including both encryption and decryption.

- A cryptographic hash function should satisfy these three assumptions:
  (A) Pre-image Resistant
  – Given y, hard to find x such that $h(x) = y$
  (B) Collision Resistant
  – Hard to find any $x \neq x'$ such that $h(x) = h(x')$
  (C) Second Pre-image Resistant
  – Given $h(x)$, hard to find x' ($\neq x$) with $h(x) = h(x')$
  Denote "$M > N$" as "M is a stronger assumption than N".

$\boxed{33}$ (2 points)
Order the strength of the assumptions (A), (B), and (C).
That is, answer in the form of "$L > M > N$".

$\boxed{34}$ (3 points)
Prove your claim of the relation between (A) and (B).

Cryptography Midterm Exam I 2007/04/16

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 □ 33 □ 34

Cryptography Midterm Exam I 2007/04/16

Solution

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

11	12	13	14	15
24	(16, 8)	(9, 5)	(0, 0)	O (Infinity)
16	17	18	19	20
(1,18)	243 (3^5)	x^2+2x+1	x^3+2x+1	22
21	22	23	24	25
416	-367	5	6	3
26	27	28	29	30
x^3+x^2+1	3	255	17	30

$\boxed{1}$ 1,0,-1,1 $\boxed{3}$ $\approx 2^{112}$ $\boxed{9}$ 120,[(12)(12345)(12)$\notin$<(12345)>],5,20 $\boxed{10}$ Profile I for software applications $\boxed{16}$ $2007P = -P$ since $4P = O$ $\boxed{18}$ $Q^{242\times5+3}=Q^3$, note $(a+b)^p=a^p+b^p$ over $\boldsymbol{F}_p$

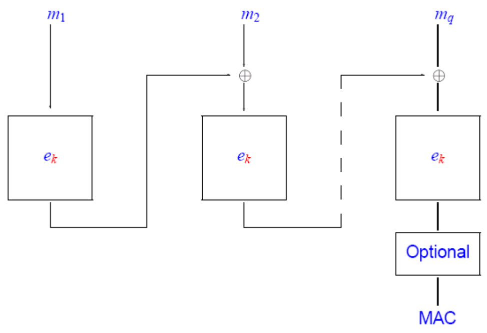
$\boxed{19}$ Extended Euclidean (GCD) algorithm: $P(x) = (x^3+x^2+2)Q(x)+(x+2)$, $Q(x) = x(x+2)+1$, so $1 = Q(x)-x(x+2) = Q(x)-x[P(x)-(x^3+x^2+2)Q(x)] = -xP(x)+ Q(x)(x^4+x^3+2x+1)$

$\boxed{20}$ min(242/2, 242/11) $\boxed{24}$ Im(h)={1,2,4,8,16} $\boxed{27}$ Shortest length of generating LFSR

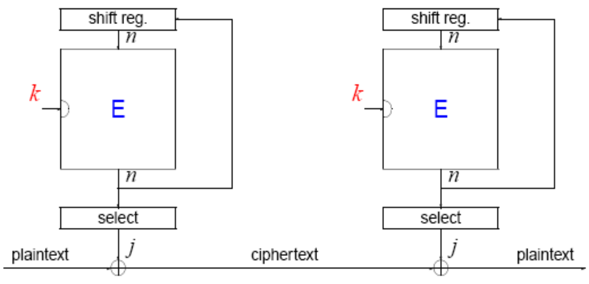
$\boxed{28}$ 2^8-1 $\boxed{29}$ 17|255 and C(x)|($x^{17}+1$)

$\boxed{33}$ $B>C>A$ $\boxed{34}$ Similar but not identical to the proof of Lemma 9.1

$\boxed{31}$



$\boxed{32}$


shift reg.
n
k
E
n
select
j
plaintext
ciphertext
shift reg.
n
k
E
n
select
j
plaintext