Cryptography Final Exam 2013/06/18

Part I (3 points each)

1. Let n be the bit length of the base field of ECC (Elliptic Curve Cryptography). What is the computational complexity of ECC? Do not confuse it with "security level".
   A. $O(n^2)$ B. $O(n^3)$ C. $O(n^4)$ D. $O(n^5)$ E. None of the above

2. Let $\sigma: GF(15625) \to GF(15625)$ be the map defined by $\sigma(x) = x^n$. Which value of n makes σ an isomorphism?
   A. 2 B. 3 C. 5 D. 6 E. None of the above

3. Let n be an RSA modulus with $n = pq$, where p and q are primes. Let e and d with $ed \equiv 1 \pmod{k}$ be public and private exponents of RSA respectively. Which is k?
   A. $pq+1$ B. $pq+p+q+1$ C. $pq-1$ D. $pq-p-q-1$ E. None of the above

4. For a secure hash function h, which should NOT be computationally infeasible?
   A. Given y, find x with $y = h(x)$ B. Given x, find x' with $x \neq x'$ and $h(x) = h(x')$
   C. Given x, find y with $y = h(x)$ D. Find x and x' with $x \neq x'$ and $h(x) = h(x')$
   E. None of the above

5. For which prime numbers p and q, a multiplicative cyclic group of order q can be constructed as a subgroup of $(\mathbf{Z}_p^*, \times)$? Typically cryptographic primitives based on the discrete logarithm problem are operated on such groups.
   A. $p = 863$, $q = 109$ B. $p = 857$, $q = 107$
   C. $p = 859$, $q = 103$ D. $p = 853$, $q = 101$ E. None of the above

6. Which should NOT be listed on a certificate?
   A. Period of validity B. Signature signed by CA
   C. Serial number D. Subject's private key E. None of the above

7. An implementation of ECC consists of four layers. Which layer is computationally most expensive and deserves most effort of optimization?
   A. Bottom layer – modular arithmetic, i.e., +, –, ×, ÷ in $GF(q)$
   B. Basic group operations, i.e., $P + Q$ and $2P$ on elliptic curve groups
   C. Scalar multiplications, i.e., kP on elliptic curve groups
   D. Upper layer – protocol, such as ECDH or ECDSA
   E. None of the above

8. Which statement about key establishment with KDC (Key Distribution Center) is FALSE?
A. Every user shares a KEK (Key Encryption Key) with KDC and each other user
B. KDC sends session keys encrypted by KEKs to users
C. In a system with *n* users, only *n* long-term key pairs are required
D. If a new user is added, a secure key is only needed between the user and the KDC
E. None of the above

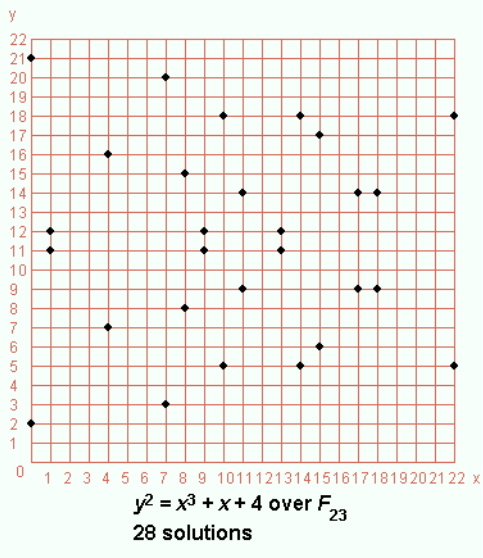
9. Which property is NOT provided by MACs (Message Authentication Codes)?
A. Fixed output length – fixed-size authentication tags are generated
B. Integrity – any manipulation of a message during transit will be detected
C. Authentication – the receiver is assured of the origin of the message
D. Non-repudiation – the sender cannot deny the origination of the message
E. None of the above

10. Which statement about DSA (Digital Signature Algorithm) is FALSE?
A. Proposed by NIST to be a Federal US Government standard
B. Based on the Elgamal signature scheme
C. Signature verification is faster compared to RSA of similar security level
D. Can be attacked if the same ephemeral key is used to sign two different messages
E. None of the above

Part II (3 points each)

- Study the structure of $GF(2^6)$
  - ♦ $GF(2^6)$ has four subfields: $GF(2)$, $GF(2^2)$, $GF(\boxed{11})$, and $GF(2^6)$ itself
  - ♦ There are $\boxed{12}$ generators of the cyclic multiplicative group $GF(2^6)^*$

- Alice and Bob will agree a key by ECDH (Elliptic Curve Diffie-Hellman key exchange) on the group defined by $y^2 = x^3 + x + 4$ over $GF(23)$. $P = (7, 3)$ is fixed as the base point.



$y^2 = x^3 + x + 4$ over F_{23}
28 solutions

  - ♦ The order of the elliptic curve group is $\boxed{13}$.
  - ♦ Alice selects $a = 21$, then sends the point $A = 21P = (10, 5)$ to Bob. Using "double-and-add" for scalar multiplication (similar to "square-and-multiply" for exponentiation), Alice needs 4 doublings and $\boxed{14}$ additions.
  - ♦ Bob selects $b = 3$, then sends the point $B = 3P = (18, 9)$ to Alice. The agreed key comes from the *x*-coordinate of the point $nP = \boxed{15}$, where $n = \boxed{16}$.

- Consider ElGamal encryption with the domain parameters $p = 47$, and $g = 4$ as a generator of the subgroup with order 23 of Z_{47}^{*}.
  - Alice's private key is $a = 3$, then her public key is $(p, g, h) = (47, 4, \boxed{17})$.
  - The ciphertext $(c_1, c_2) = (37, 12)$ is obtained from Bob, where $c_1 = g^k \bmod p$ and k is a random ephemeral key chosen by him. Then the corresponding plaintext is $m = \boxed{18}$.

- SHA (Secure Hash Algorithm) standards are published by NIST.
  - The output length of SHA-1 is $\boxed{19}$ bits. The research led by Xiaoyun Wang reduced the complexity of finding a collision from 2^{80} to 2^{63}.
  - SHA-2 has four possible output lengths: 224, $\boxed{20}$ $(=m)$, $\boxed{21}$ $(=n)$, and 512 bits. According to Suite B announced by NSA (National Security Agency), SHA-m and SHA-n are used to protect classified information up to Secret and Top Secret levels of US government respectively.
  - SHA-3 competition was won by Keccak algorithm in October, 2012.

- Complete the Left-to-Right Square-and-Multiply for modular exponentiation:

  INPUT: x, modulus n, and $k = (k_t, \ldots, k_1, k_0)_2$ with $k = \sum_{i=0}^{t} k_i 2^i$ where $k_i \in \{0, 1\}$

  OUTPUT: $x^k \bmod n$

```
1. $r \leftarrow x$
2. For $i$ from $\boxed{22}$ downto 0 do
    2.1  $r \leftarrow r^2 \bmod n$
    2.2  If $k_i = 1$ then $r \leftarrow \boxed{23} \bmod n$
3. Return ($r$)
```

- Miller-Rabin primality test is extensively used for prime generations.
  - The test is based on the following fact:

    If $a \neq \pm 1 \pmod{n}$ but $\boxed{24} \pmod{n}$, then n must be a composite.
  - Complete the Miller-Rabin test to determine the primality of an integer n:

```
Write $n-1 = 2^k m$ where $m$ is odd
Choose $a \in \{2, \ldots, n-2\}$ randomly
Compute $b = \boxed{25} \pmod{n}$
If $(b \neq 1$ and $b \neq (n-1))$
    $i = 1$
    While $(i < k$ and $b \neq (n-1))$
        $b = \boxed{26} \pmod{n}$
        If $(b = 1)$ Output (Composite, $a$)
        $i = i + 1$
    If $(b \neq (n-1))$ Output (Composite, $a$)
Output "Probable Prime"
```

- RSA decryption is usually performed with Chinese Remainder Theorem (CRT). Suppose Bob has public modulus $N = 221$ ($= 13 \times 17$) with prime factors $p = 13$ and $q = 17$ kept secret, and public exponent $e = 5$ for encryption.
    - The value of Euler ϕ-function for N is $\phi(221)$ = $\boxed{27}$.
    - Bob's private key for decryption is d = $\boxed{28}$, where $0 < d < \phi(221)$.
    - The ciphertext $c = 73$ sent by Alice is decrypted by Bob as follows.
        - $c^d \bmod p = (c \bmod p)^{d \bmod \phi(p)} \bmod p = 8 = A$, where $0 \le A < p$.
        - $c^d \bmod q = (c \bmod q)^{d \bmod \phi(q)} \bmod q =$ $\boxed{29}$ $= B$, where $0 \le B < q$.
        - Solving the system of equations $c^d \equiv A \pmod{p}$ & $c^d \equiv B \pmod{q}$ by CRT, Bob obtains the plaintext $m = c^d \bmod N =$ $\boxed{30}$, where $0 \le m < N$. This answer can be double-checked by the equality $c \equiv m^e \pmod{N}$.

Part III (Write down all details of your work)

$\boxed{31}$ (4 points)

Apparently there are two irreducible polynomials of degree one over $GF(2)$: x and $x+1$. Answer the following questions.

(a) How many monic irreducible polynomials of degree 1 over $GF(2^2)$?

(b) How many monic irreducible polynomials of degree 2 over $GF(2^2)$?

(c) How many irreducible polynomials of degree 5 over $GF(2)$?

(d) How many irreducible polynomials of degree 10 over $GF(2)$?

$\boxed{32}$ (6 points)

Let n be the output length in bit of a hash function h, and t mutually distinct message $(x_1, x_2, \ldots, x_t)$ be randomly selected to test collision $h(x_i)=h(x_j)$.

(a) What is the probability for no collision among t hash values?

(b) What is the Taylor series at 0 for the function $f(x) = e^{-x}$?

(c) Denote the probability of "at least one collision" by $\lambda = 1 - P(\text{no collision})$. Use the linear approximation of e^{-x} to deduce that

$$t \approx 2^{(n+1)/2} \sqrt{\ln\left(\frac{1}{1-\lambda}\right)}$$

Cryptography Final Exam 2013/06/18

Name: _____________ Student ID number: _____________

<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></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></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"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></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"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></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"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></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"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

31 & 32

Cryptography Final Exam 2013/06/18

Solution

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

11	12	13	14	15
8 (or 2^3)	36	29	2	(1, 12)
16	17	18	19	20
5 (or 63)	17	28	160	256
21	22	23	24	25
384	$t-1$	$r\,x$	$a^2 \equiv 1$	a^m
26	27	28	29	30
b^2	192	77	3	190

31

(a) 4 (b) 6 (c) $\frac{2^5-2}{5}=6$ (d) $\frac{2^{10}-2^5-2^2+2}{10}=99$

32