Cryptography Midterm Exam II 2007/06/11

Part I (3 points each)

1. Apply Fermat's primality test on 15. Which is NOT a *witness of compositeness*?
   A. 2 B. 4 C. 7 D. 8 E. None of the above

2. Assuming the 160-bit security for the group order on elliptic curves, which is the message size for the *signed* Diffie-Hellman protocol (EC-DH + EC-DSA)?
   A. 160 B. 320 C. 480 D. 640 E. None of the above

3. To compute $(x_1 2^{32} + x_0) \times (y_1 2^{32} + y_0)$ with Karatsuba multiplication where x_0, x_1, y_0, and y_1 are 32-bit numbers, which multiplication is not necessary to perform?
   A. $x_1 \times y_1$ B. $x_0 \times y_1$ C. $x_0 \times y_0$ D. $(x_0 + x_1) \times (y_0 + y_1)$ E. None of the above

4. Which algorithm for solving the discrete logarithm problem has *sub-exponential* time complexity?
   A. Index-calculus B. Pohlig-Hellman
   C. Baby-Step/Giant-Step D. Pollard's ρ method E. None of the above

5. Which property is not provided by digital signature schemes?
   A. Message integrity B. Authentication C. Non-repudiation
   D. Message confidentiality E. None of the above

6. Which hard problem is the security of the ElGamal encryption based on?
   A. Graph isomorphism B. Integer factoring C. Discrete logarithm
   D. Square root modulo a composite E. None of the above

7. Given an abelian group $(G, \times)$ and $g \in G$, consider the following problems.
   - DDH : Given $a = g^x$, $b = g^y$, $c = g^z$. Determine if $z = xy$.
   - DHP : Given $a = g^x$ and $b = g^y$. Find $c = g^{xy}$.
   - DLP : Given $h \in G$ such that $h = g^x$. Find x.

   $A \leq_P B$ means "A is reducible to B in polynomial time".
   Which relation is correct?
   A. DDH $\leq_P$ DLP $\leq_P$ DHP
   B. DHP $\leq_P$ DLP $\leq_P$ DDH
   C. DHP $\leq_P$ DDH $\leq_P$ DLP
   D. DLP $\leq_P$ DDH $\leq_P$ DHP
   E. None of the above

8. Which statement is FALSE about PKI?
   A. PGP aims to provide channel security to fulfill commercial requirement
   B. X509 defines a structure for public key certificates
   C. CRL is a list of the serial numbers of all the revoked certificates
   D. RA established the identity of users, but does not sign certificates
   E. None of the above

9. Which statement is FALSE about digital signature schemes?
   A. Schnorr signature scheme has provable security
   B. Nyberg–Rueppel scheme has the property of message recovery
   C. Hash functions make signature schemes efficient for long messages
   D. To achieve the same security level, DSA on prime fields has better efficiency than EC-DSA on elliptic curves
   E. None of the above

10. Which statement is FALSE about Identity Based Cryptography?
   A. Its first signature scheme is based on the discrete logarithm problem
   B. Its first encryption scheme is based on bilinear pairing on elliptic curves
   C. It removes the need for storage and transmission of certificates
   D. It does not remove the need for a trusted third party
   E. None of the above

Part II (3 points each)

- The ciphertext $c = 66$ was encrypted by the Rabin public-key cryptosystem $c = m \times (m + 20) \pmod{221}$. All four possible corresponding plaintexts are $m = 49$, 100, [11], and [12] (increasing order).

- Consider the Diffie-Hellman key exchange scheme on $\boldsymbol{Z}_{19}$ with the generator $g = 2$. If Alice sent Bob 16 and the agreed key was 17, what did Bob send Alice? There are two possibilities: [13] and [14].

- Miller-Rabin primality test
  - The test is based on this fact: If $a \neq \pm 1 \pmod{n}$ but [15] $\pmod{n}$, then n must be a composite.
  - To generate a large prime, Miller-Rabin test should be repeated on a candidate integer at least [16] times to make sure the error probability $\leq 10^{-9}$.

- Fast modular exponentiation:
  - $18^{2007} \bmod 23 =$ [17].
  - $524^{2007} \bmod 667 =$ [18]. (Need some tricks speeding up RSA decryptions)

- $N = 40741 = p \times q$ has the value of Euler ϕ-function $\phi(N) = 40300$.
  - Assume the prime factors $p > q$, then $p =$ [19].
  - If N is used as an RSA modulus and the public exponent $e = 3$, then the private exponent $d =$ [20].

- $N = 43739 = p \times q$ satisfies:
$$296^2 \equiv 138 = 2 \times 3 \times 23 \pmod{N}$$
$$302^2 \equiv 3726 = 2 \times 3^4 \times 23 \pmod{N}$$
$$305^2 \equiv 5547 = 3 \times 43^2 \pmod{N}$$
$$363^2 \equiv 552 = 2^3 \times 3 \times 23 \pmod{N}$$
$$373^2 \equiv 7912 = 2^3 \times 23 \times 43 \pmod{N}$$
  - To factor N, we compute $\gcd(a, N)$ which is likely to be a proper factor of N, where $a =$ [21] is derived from the above relations.
  - Assume the prime factors $p > q$, then $p =$ [22].

- Let $\boldsymbol{A}$ be a 4×4 invertible matrix over $\boldsymbol{Z}_7$ with the minimal polynomial $x^4 + 6x^3 + 2x + 4$.
  - Suppose $5\boldsymbol{A}^{2007} + 2\boldsymbol{A}^{2006} + 3\boldsymbol{A}^{2004} + c\boldsymbol{A}^{2003} = \boldsymbol{0}$. Then $c =$ [23].
  - $\boldsymbol{b}$ and $\boldsymbol{x}$ are two column vectors satisfying $\boldsymbol{Ax} = \boldsymbol{b}$. Expressing $\boldsymbol{x}$ in terms of $\boldsymbol{b}$ and $\boldsymbol{A}^i$ with $i > 0$, we have $\boldsymbol{x} = 5\boldsymbol{A}^3\boldsymbol{b} +$ [24].

- Perform XL algorithm to solve a system of 10 quadratic equations in 7 variables. Select $D = 4$ to be the degree to reach. Multiply every equation by all possible monomials of degree ≤ 2.
  - Now the number of equations is $R =$ [25].
  - The number of monomials of total degree ≤ D is $T =$ [26].

- Suppose a user wishes to be authenticated to a building with a smart card which performs Schnorr signature scheme. Let $G = \langle g \rangle$ be a group of prime order q. Let x be the secret key and $y = g^x$ be the public key. Denote the card as C and the card reader as R. Then the protocol is:
  - [Commitment] $C \rightarrow R$: $r = g^k$ where k is random
  - [Challenge] $R \rightarrow C$: a random value m
  - [Response] $C \rightarrow R$: $s =$ [27] (mod q)
  - [Verification] C accepts the signature s if $r =$ [28]

- Solve $5^x \equiv 219 \pmod{307}$ with Baby-Step/Giant-Step algorithm. Derived from the tables below, the solution is $x =$ 29 $(0 < x < 307)$ corresponding to $k =$ 30. Here we have $5^{-18} \equiv 235 \pmod{307}$.

Baby steps:

i	0	1	2	3	4	5	6	7	8
5^i	1	5	25	125	11	55	275	147	121
i	9	10	11	12	13	14	15	16	17
5^i	298	262	82	103	208	119	288	212	139

Giant steps:

k	0	1	2	3	4	5	6	7	8
219×5^{-18k}	219	196	10	201	264	26	277	11	129
k	9	10	11	12	13	14	15	16	17
219×5^{-18k}	229	90	274	227	234	37	99	240	219

Part III (Write down all details of your work)

31 (6 points)

Consider the following commitment scheme:

- $G = < g >$ is a group of prime order q
- $h = g^x \in G$ but neither Alice nor Bob knows x
- To commit to a value $a \in \{0, \ldots, q-1\}$, Alice generates $b \in \{0, \ldots, q-1\}$ at random and computes $c = g^a h^b$
- To reveal the commitment, Alice sends Bob a and b

(1) Is the scheme *Perfectly Binding* or *Computationally Binding*? Explain your answer.

(2) Is the scheme *Perfectly Concealing* or *Computationally Concealing*? Explain your answer.

32 (4 points)

Suppose the public exponent $e = 3$ is used by three users with the public moduli N_1, N_2, and N_3. If somebody else encrypts the same message m and sends the ciphertext c_1, c_2, and c_3 to them respectively, explain how an attacker can obtain the plaintext m from the above ciphertext and the public information.

Cryptography Midterm Exam II 2007/06/11

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

Cryptography Midterm Exam II 2007/06/11

Solution

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

11	12	13	14	15
101	152	5	14	$a^2 \equiv 1$

16	17	18	19	20
15	3	26	311	26867

21	22	23	24	25
107172	229	6	$2\boldsymbol{A}^2\boldsymbol{b} + 3\boldsymbol{b}$	360

26	27	28	29	30
330	$k + mx$	$g^s y^{-m}$	130	7

1 $2^{15-1} \equiv 7^{15-1} \equiv 8^{15-1} \equiv 4$ while $4^{15-1} \equiv 1 \pmod{15}$ 7 DDH $\leq_P$ DHP $\leq_P$ DLP 11 12 $m \equiv 15,16 \pmod{17}$ and $m \equiv 9,10 \pmod{13}$ 21 $(296 \times 363)^2 \equiv (2^2 \times 3 \times 23)^2 \pmod{N}$, gcd (107448−276, N) = 229. Other reasonable answers such as 107724, 19694, … are also accepted.

25 $10 \times C_{4-2}^{4+7-2}$ 26 $H_4^{7+1} = C_4^{4+7}$ 31 Computationally Binding, Perfectly Concealing