Cryptography Midterm Exam II 2008/06/02

Part I (3 points each)

1. For RSA modulus $N = 10403 = 101\times103$, which can NOT be a public exponent e?
   A. 11 B. 13 C. 17 D. 19 E. None of the above

2. Apply Fermat's primality test on 21. Which is NOT a *witness of compositeness*?
   A. 2 B. 4 C. 5 D. 8 E. None of the above

3. What is the output length (in bits) of the hash function SHA-1?
   A. 128 B. 144 C. 160 D. 192 E. None of the above

4. The *branch number* in the case of MixColumn operation of AES is defined by $\min_{\boldsymbol{a}\neq\mathbf{0}}(\mathrm{W}(\boldsymbol{a})+\mathrm{W}(F(\boldsymbol{a})))$, where $\boldsymbol{a}$ is a 4-byte vector, F is a linear transformation, and W is the weight function. What is the maximal branch number?
   A. 5 B. 6 C. 7 D. 8 E. None of the above

5. Apply the Miller-Rabin test t times to an odd composite number. Which is the best estimate of the probability of finding at least one *witness of compositeness*?
   A. $(\frac{1}{2})^t$ B. $(\frac{3}{4})^t$ C. $1-(\frac{3}{4})^t$ D. $1-(\frac{1}{2})^t$ E. $1-(\frac{1}{4})^t$

6. Which item is definitely NOT listed on a certificate? A. Public key
   B. Private key C. User name D. Expiry date E. None of the above

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

8. Which statement is FALSE about Merkle-Damgård construction of hash functions?
   A. Use a collision-resistant compression function f with arbitrary length of input
   B. Add a single one bit to signal the end of a message, then pad with zeros
   C. The final block encodes the original length of the unpadded message in bits
   D. The internal state $H := f(H \,||\, m_i)$ is updated repeatedly with message block m_i
   E. None of the above

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

10. 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". Which relation is correct?
A. (c) > (b) > (a) B. (b) > (a) > (c) C. (a) > (c) > (b)
D. (c) > (a) > (b) E. None of the above

Part II (3 points each)

- Represent $\boldsymbol{F}_{16}$ by polynomial representations with the irreducible $f(x) = x^4 + x + 1$. Choosing $g = (0010)$ as a generator for $\boldsymbol{F}_{16}$, we list all elements of $\boldsymbol{F}_{16}$ as follows.

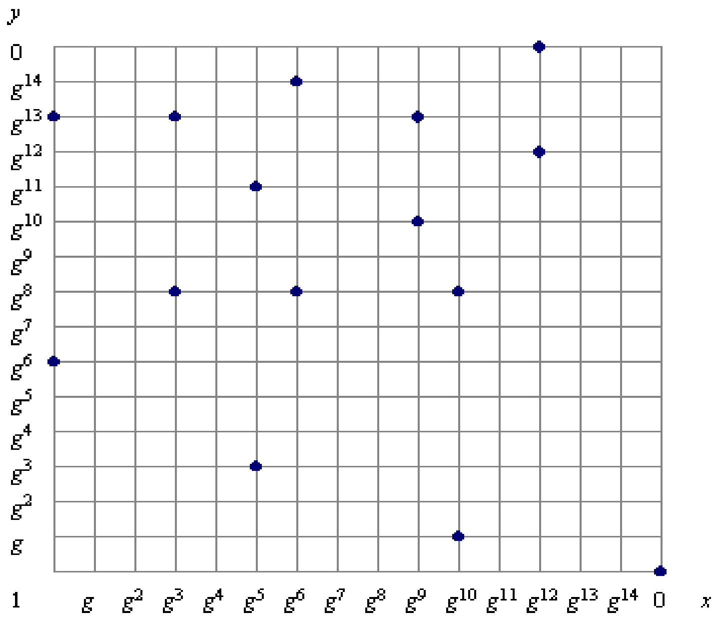
$0 = (0000)$	$g^0 = (0001)$	$g^1 = (0010)$	$g^2 = (0100)$
$g^3 = (1000)$	$g^4 = (0011)$	$g^5 = (0110)$	$g^6 = (1100)$
$g^7 = (1011)$	$g^8 = (0101)$	$g^9 = (1010)$	$g^{10} = (0111)$
$g^{11} = (1110)$	$g^{12} = (1111)$	$g^{13} = (1101)$	$g^{14} = (1001)$

Consider the elliptic curve group G defined by $y^2 + xy = x^3 + g^4 x^2 + 1$ over $\boldsymbol{F}_{16}$.
There are 15 points satisfying the equation as the graph.

Let $P = (1, g^6)$ and $Q = (g^5, g^{11})$.

- The group order $|G| = \boxed{11}$.
- $P + Q = \boxed{12}$.
- $-Q = \boxed{13}$.
- $2P = \boxed{14}$.
- $4P = \boxed{15}$.

The formulas in Part III might help your computations.



- Factor $n = 87463$ with the Quadratic Sieve. Define $g(x) = x^2 - n$.

x	-1	2	3	13	17	19	29
265	1	1	1	0	1	0	0
278	1	0	1	1	0	0	1
296	0	0	0	0	1	0	0
299	0	1	1	0	1	1	0
307	0	1	0	1	0	0	1
316	0	0	0	0	1	0	0

x	2	3	13	17	19	29	$x^2 - n$ splits
261	X				X		
262		X		X			
263	X	X					
264							
265	X	X	X	X			$-2 \cdot 3 \cdot 13^2 \cdot 17$
266		X					
267	X						
268		X	X				
269	X	X					
270							
271	X	X			X		
272		X					
273	X					X	
274		X					
275	X	X					
276							
277	X	X					
278		X	X			X	$-3^3 \cdot 13 \cdot 29$
279	X			X			
280		X			X		

x	2	3	13	17	19	29	$x^2 - n$ splits
296		X		X			$3^2 \cdot 17$
297	X						
298		X					
299	X	X		X	X		$2 \cdot 3 \cdot 17 \cdot 19$
300							
301	X	X					
302		X				X	
303	X						
304		X	X				
305	X	X					
306							
307	X	X	X			X	$2 \cdot 3^2 \cdot 13 \cdot 29$
308		X					
309	X				X		
310		X					
311	X	X					
312							
313	X	X		X			
314		X					
315	X						
316		X		X			$3^6 \cdot 17$

The integers x_1, x_2, and b satisfy
$g(265) \times g(278) \times g(x_1) \times g(x_2) \equiv b^2 \pmod{n}$.

- If $0 < x_1 < x_2$, then $x_2 =$ $\boxed{16}$.
- If $0 < b < n$, then $b =$ $\boxed{17}$.
- If $a \equiv 265 \times 278 \times x_1 \times x_2 \pmod{n}$ and $0 < a < n$, then $a =$ $\boxed{18}$.
- If $n = p \times q$ and $0 < p < q$, then $p =$ $\boxed{19}$ and $q =$ $\boxed{20}$.

These congruences might reduce your computational effort:
$265 \times 307 = 81355 \equiv -6108 \pmod{n}$
$265 \times 316 = 83740 \equiv -3723 \pmod{n}$
$278 \times 296 = 82288 \equiv -5175 \pmod{n}$
$278 \times 299 = 83122 \equiv -4341 \pmod{n}$
$3^5 \times 13 \times 17 \times 29 \equiv -16947 \pmod{n}$
$3^4 \times 13^2 \times 17 \times 29 \equiv 14026 \pmod{n}$

- The solution to the system of congruences

$$2x \equiv 3 \pmod{7} \qquad 3x \equiv 6 \pmod{11} \qquad 4x \equiv 10 \pmod{13}$$

is $x \equiv$ $\boxed{21}$ (mod $\boxed{22}$)

- Consider the RSA signature scheme with the public key $n = 85$ and $e = 3$.
  - The private key for signing is $d =$ $\boxed{23}$.
  - Signing the message $m = 4$, a user obtains its digital signature $s =$ $\boxed{24}$.

- In a Diffie-Hellman key exchange scheme on $\boldsymbol{Z}_{31}$ with the generator $g = 3$, Alice chooses 9 and Bob chooses 7 in private. Then Alice sends $\boxed{25}$ to Bob, and the agreed key is $\boxed{26}$.

- Decrypting the ciphertext $c = 39$ of the Rabin public-key cryptosystem $c = m \times (m + 10) \pmod{187}$, a user obtains four possible corresponding plaintexts $m = 3, 20,$ $\boxed{27}$, and $\boxed{28}$ (in increasing order).

- If a message m is divided into t blocks $m_1, m_2, \ldots, m_t$, then the CBC-MAC with a cipher e and a key k is derived by the process $I_1 = m_1$, $O_1 = e_k(I_1)$, $I_i = m_i \oplus \boxed{29}$, and $O_i = \boxed{30}$ for $i = 2, 3, \ldots, t$.

Part III (Write down all details of your work)

$\boxed{31}$ (5 points)

Derive arithmetic formulas of elliptic curve groups defined by $y^2 + xy = x^3 + ax^2 + b$ with $b \neq 0$ over $\boldsymbol{F}_{2^m}$.

(a) $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two distinct points on the curve with $P_1 \neq -P_2$. If $(x_3, y_3) = P_1 + P_2$ and $s = (y_1 + y_2)/(x_1 + x_2)$, show that $x_3 = s^2 + s + x_1 + x_2 + a$ and $y_3 = s(x_1 + x_3) + x_3 + y_1$.

(b) $P_0 = (x_0, y_0)$ is a point on the curve with $x_0 \neq 0$. If $(x_4, y_4) = 2P$, show that $x_4 = x_0^2 + (b/x_0^2)$ and $y_4 = x_0^2 + x_4(y_0/x_0 + x_0 + 1)$.

$\boxed{32}$ (5 points)

As the MixColumn operation of AES, we work on polynomials of degree 3 over $\boldsymbol{F}_{256}$. Let $a(x) = a_3(x+1)^3 + a_2(x+1)^2 + a_1(x+1) + a_0$ and $b(x) = b_3(x+1)^3 + b_2(x+1)^2 + b_1(x+1) + b_0$ be two polynomials with a_i, b_i in $\boldsymbol{F}_{256}$.

(a) If $a(x)\,b(x) \equiv 1 \pmod{(x^4 + 1)}$, show that

(i) $b_0 = a_0^{-1}$

(ii) $b_1 = a_1\, b_0\, a_0^{-1}$

(Also $b_2 = (a_2\, b_0 + a_1 b_1)\, a_0^{-1}$ and $b_3 = (a_3\, b_0 + a_2\, b_1 + a_1 b_2)\, a_0^{-1}$, but you do not have to show them.)

(b) Find all *self-inverse* polynomials. That is, indicate the conditions on $a(x)$ such that $a(x)^2 \equiv 1 \pmod{(x^4 + 1)}$. Prove your claim.

Cryptography Midterm Exam II 2008/06/02

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 II 2008/06/02

Solution

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

11	12	13	14	15
16	(g^{10}, g^8)	(g^5, g^3)	(0, 1)	O (Infinity)
16	**17**	**18**	**19**	**20**
307 (316)	28052 (77542)	34757 (9921)	149	587
21	**22**	**23**	**24**	**25**
607	1001	43	64	29
26	**27**	**28**	**29**	**30**
27	157	174	O_{i-1}	$e_k(I_i)$

32

(b) $a(x) = a_3(x+1)^3 + a_2(x+1)^2 + 1$ with a_3, a_2 in $\boldsymbol{F}_{256}$,

or $a(x) = b_3 x^3 + b_2 x^2 + b_3 x + (b_2 + 1)$ with b_3, b_2 in $\boldsymbol{F}_{256}$.