Cryptography   Midterm Exam   2009/04/14

Part I   (3 points each)

1. For a group homomorphism f: $(\mathbf{Z}_{10}, + \bmod 10) \rightarrow (\mathbf{Z}_{11}^*, \times \bmod 11)$, which assignment of the value of $f(1)$ makes f an *isomorphism*?
   A. 3   B. 5   C. 7   D. 9   E. None of the above

2. For RSA modulus $N = 4087 = 61 \times 67$, which can NOT be a public exponent e?
   A. 11   B. 13   C. 17   D. 19   E. None of the above

3. Which group is isomorphic to the Klein-4 group $(\mathbf{Z}_8^*, \times)$?
   A. $(\mathbf{Z}_4, +)$ B. $(\mathbf{Z}_5^*, \times)$ C. $(\mathbf{Z}_{10}^*, \times)$ D. $(\mathbf{Z}_{12}^*, \times)$ E. None of the above

4. Which multiplicative group is NOT of order 12?
   A. $\mathbf{Z}_{13}^*$ B. $\mathbf{Z}_{21}^*$ C. $\mathbf{Z}_{28}^*$ D. $\mathbf{Z}_{36}^*$ E. None of the above

5. Which is a *normal basis* of GF(2^5) over GF(2) with $t \in$GF(2^5)?
   A. $\{1, t, t^2, t^3, t^4\}$ B. $\{t, t^2, t^4, t^6, t^8\}$
   C. $\{1, t, t^2, t^4, t^8\}$ D. $\{t, t^2, t^4, t^8, t^{16}\}$ E. None of the above

6. Which quotient ring is isomorphic to $GF(2^5)$?
   A. $GF(2)[x]/<x^5 + x^2 + 1>$ B. $GF(2)[x]/<x^5+x^3+x^2+1>$
   C. $GF(2)[x]/<x^5 + x + 1>$ D. $GF(2)[x]/<x^5+x^3+x+1>$ E. None of the above

7. Which irreducible polynomial is *primitive* over $GF(2)$?
   A. $x^6+x^5+x^4+x^2+1$ B. $x^6 + x^3 + 1$
   C. $x^6+x^4+x^2+x+1$ D. $x^6 + x + 1$ E. None of the above

8. A cipher E encrypts 6 hexadecimal digits in the way of E(123456) = 416235 and E(1C5A3F) = A1FC53. Which category does this cipher belong to?
   A. Substitution cipher   B. Permutation cipher
   C. Vigenère cipher   D. Shift cipher   E. None of the above

9. Which assumption ensures the security of ElGamal encryption against chosen plaintext attacks?   A. Discrete Logarithm Problem is hard
   B. Square Root Problem is hard   C. Diffie-Hellman Problem is hard
   D. Factoring Problem is hard   E. None of the above

10. Which is NOT proved or disproved yet about Rabin or RSA encryption schemes with modulus $n = pq$, public exponent e, and private exponent d?
A. Breaking Rabin encryption is equivalent to factoring n
B. Breaking RSA encryption is equivalent to factoring n
C. Knowing d is equivalent to factoring n
D. Knowing $\varphi(n)$ is equivalent to factoring n
E. None of the above

Part II (3 points each)

- $x \equiv \boxed{11}$ (mod $\boxed{12}$) is the solution to the system of congruences
  $4x \equiv 1 \pmod{7}$ $\quad$ $5x \equiv 4 \pmod{9}$ $\quad$ $6x \equiv 9 \pmod{11}$

- The prime numbers $p = \boxed{13}$ and $q = \boxed{14}$ with $p > q$ satisfy $n = p \times q = 43423$ and $\phi(n) = 43000$.

- In the multiplicative group ($\mathbf{Z}_{33}^*$, ×):
  - 26^{-1} (the multiplicative inverse of 26) = $\boxed{15}$.
  - $o(4)$ (the order of 4) = $\boxed{16}$.

- $\mathrm{GL}_2(Z_{13})$ is the group of invertible 2 × 2 matrices with entries in Z_{13}, and $\mathrm{SL}_2(Z_{13})$ is its subgroup consisting of the matrices with determinant 1. Their group orders are $|\mathrm{GL}_2(Z_{13})| = \boxed{17}$ and $|\mathrm{SL}_2(Z_{13})| = \boxed{18}$.

- Complete the following algorithm of scalar multiplication on a given elliptic curve group. It is similar to the right-to-left square-and-multiply exponentiation.

  INPUT: a point P on the curve, a positive integer $k = (k_{t-1}, \ldots, k_1, k_0)_2$
  OUTPUT: the point kP on the curve

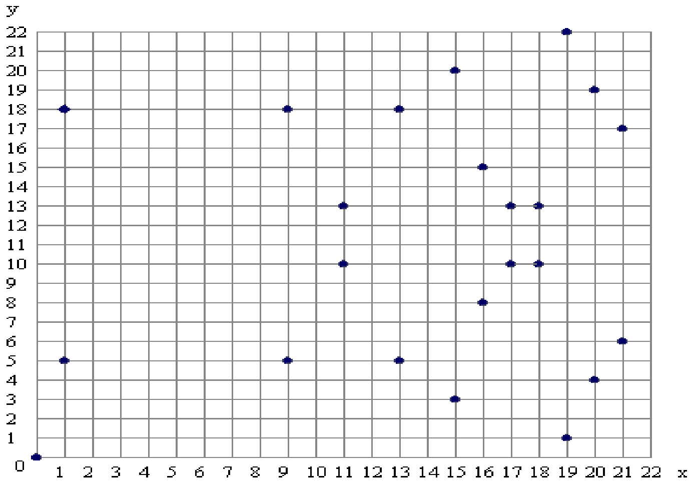
```
1.  $R \leftarrow \infty$   ($O$: point at infinity)
2.  For $i$ from 0 to $t-1$ do
    2.1  If $k_i = 1$ then $R \leftarrow \boxed{19}$
    2.2  $P \leftarrow \boxed{20}$
3.  Return ($R$)
```

- Consider RSA encryption with the public key $n = 187$ and $e = 3$.
  - The private key for decryption is $d = \boxed{21}$.
  - The ciphertext $c = \boxed{22}$ is obtained by encrypting the message $m = 11$.

- 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 $(p, g, h) = (47, 4, \boxed{23})$.
  - The ciphertext $(c_1, c_2) = (37, 11)$ 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 $m = \boxed{24}$.

- Break the Hill cipher with a known-plaintext attack. Its encryption is defined by $\boldsymbol{c} = \boldsymbol{pM} \bmod 5$, where $\boldsymbol{M} \in \mathrm{GL}_2(Z_5)$, $\boldsymbol{p} = [p_1\ p_2]$ and $\boldsymbol{c} = [c_1\ c_2]$ are plaintext and ciphertext respectively.
  - Two known pairs of plaintexts and ciphertexts $\boldsymbol{p}_1 = [1\ 4] \mapsto \boldsymbol{c}_1 = [1\ 1]$ and $\boldsymbol{p}_2 = [3\ 0] \mapsto \boldsymbol{c}_2 = [1\ 2]$ are obtained. Then $\boldsymbol{M} = \boxed{25}$.
  - Suppose the a ciphertext $\boldsymbol{c}_3 = [1\ 0]$ is intercepted. Then the corresponding plaintext is $\boldsymbol{p}_3 = \boxed{26}$.

- 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. Let $P = (18, 10)$ and $Q = (19, 1)$.
  - The order of the elliptic curve group is $\boxed{27}$.
  - $P - Q = \boxed{28}$.
  - $3P = \boxed{29}$.
  - $2009P = \boxed{30}$.



Part III (Write down all details of your work)

$\boxed{31}$ (4 points)

Over $GF(3)$, suppose $p(x) = x^3 + 2x^2 + x + 2$ and $q(x) = x^4 + 2x^3 + 2x^2 + 1$. Write $\gcd(p(x), q(x))$ as a monic polynomial, i.e., the leading coefficient is 1. Find polynomials $f(x)$ and $g(x)$ such that $f(x)p(x) + g(x)q(x) = \gcd(p(x), q(x))$.

$\boxed{32}$ (3 points)

Show that using a small public exponent for RSA may not be secure as follows. Suppose the public exponent $e = 3$ is taken 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.

33 (3 points)

Show that RSA is not secure against (*adaptive*) *chosen ciphertext attacks* as follows. Suppose the message m that Eve wants to break is from $c = m^e \pmod{N}$. Eve creates the 'related' ciphertext $c' = 2^e c$ and asks an oracle to decrypt c' to give m'. Express m in terms of what Eve has obtained and prove your answer.

Cryptography Midterm Exam 2009/04/14

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

Cryptography Midterm Exam 2009/04/14

Solution

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

11	12	13	14	15
359	693	251	173	14
16	17	18	19	20
5	168×156 $(= 26208)$	168×13 $(= 2184)$	$P + R$	$2P$
21	22	23	24	25
107	22	17	10	$\begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix}$
26	27	28	29	30
$[4 \quad 3]$	24	(15, 3)	Point at Infinity $(O,\ \infty)$	(18, 13)

$\boxed{31}$ gcd $= x + 2$, $f(x) = 2x^2 + 2x + 2$, $g(x) = x + 1$

$\boxed{33}$ $m = m'/2 \bmod N$