Cryptography Final Exam 2012/06/19

Part I (3 points each)

1. To compute a^{43} by "Square-and-Multiply", how many "Multiply" are required?
A. 3 B. 4 C. 5 D. 6 E. None of the above

2. For RSA modulus $N = 185617 = 419 \times 443$, which is a possible public exponent e?
A. 11 B. 13 C. 17 D. 19 E. None of the above

3. Which is a generator of a cyclic multiplicative group of order 5 in $\boldsymbol{Z}_{41}$*?
A. $3^{(41-1)/5}$ B. $9^{(41-1)/5}$ C. $14^{(41-1)/5}$ D. $32^{(41-1)/5}$ E. None of the above

4. Which is NOT a legitimate output length of the family of SHA-2 hash functions?
A. 128 B. 256 C. 384 D. 512 E. None of the above

5. Which hash function is a first-round candidate of the SHA-3 competition, but is NOT selected to advance to the third (final) round?
A. Skein B. Grøstl C. Keccak D. MD6 E. BLAKE

6. Which service is provided by digital signature schemes but NOT by message authentication codes? A. Message authentication B. Message integrity
C. Non-repudiation D. Message confidentiality E. None of the above

7. A cryptographic hash function should satisfy these three assumptions:
(a) Collision Resistant – Hard to find any $x \neq x'$ such that $h(x) = h(x')$
(b) Pre-image Resistant – Given y, hard to find x such that $h(x) = y$
(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. (a) > (c) > (b)
C. (c) > (a) > (b) D. (a) > (b) > (c) E. None of the above

8. According to Prof. Ron Rivest, which can be described as "I can convince you that I know a solution to a hard problem while telling you nothing about my solution even if you are very skeptical"?
A. Random oracle B. Homomorphic encryption
C. Oblivious transfer D. Zero-knowledge proof E. None of the above

9. Which statement is FALSE about RC4?
   A. The most widely-used software stream cipher
   B. Its internal state is an array of 128 bytes
   C. Its internal state evolves in an unpredictable and non-linear way
   D. Known attacks can be defended by discarding the initial portion of the keystream
   E. None of the above

10. Which is NOT proved or disproved yet about RSA with modulus $n = pq$, public exponent e, and private exponent d?
    A. Knowing d is equivalent to factoring n
    B. Knowing $\phi(n)$ is equivalent to factoring n
    C. Breaking RSA is equivalent to factoring n
    D. Secure against chosen plaintext attack assuming the RSA-Problem is hard
    E. None of the above

Part II (3 points each)

- The RSA signature scheme performed with Chinese Remainder Theorem (CRT) is implemented in many low-cost chips. Suppose $p = 11$ and $q = 29$ are kept private, and the public modulus is $n = 319 = 11 \times 29$.
  - The value of Euler ϕ-function for n is $\phi(319) = \boxed{11}$.
  - If the public exponent for verification is $e = 3$, the corresponding private key for signing is $d = \boxed{12}$, where $0 < d < \phi(319)$.
  - Sign the message $m = 89$ by CRT as follows.
    - $m^d \bmod p = (m \bmod p)^{d \bmod \phi(p)} \bmod p = \boxed{13} = A$, where $0 \le A < p$.
    - $m^d \bmod q = (m \bmod q)^{d \bmod \phi(q)} \bmod q = \boxed{14} = B$, where $0 \le B < q$.
    - Solve the system of equations by CRT: $m^d \equiv A \pmod{p}$; $m^d \equiv B \pmod{q}$. The digital signature of m is $S = m^d \bmod n = \boxed{15}$, where $0 \le S < n$.
  - Verify the signature S as follows.
    - Compute $m' = \boxed{16}$ mod n. (Fill in a formula related to S and e)
    - If $m = m'$, then the digital signature S is accepted. Otherwise S is rejected.

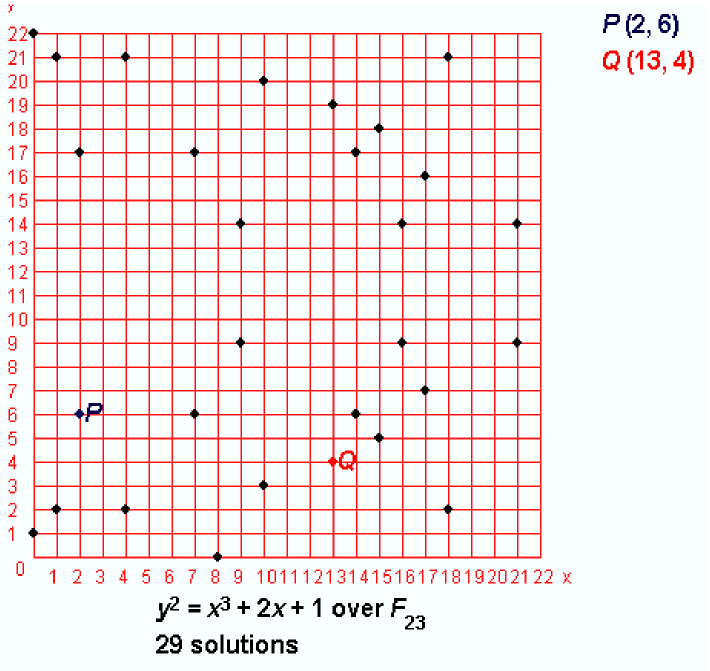
    Note that the correctness of your answers to the values of A, B, and S can be confirmed in a similar way.

- Assume the periodic sequence 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, … of period 7 is generated by an LFSR (Linear Feedback Shift Register).
  - The connection polynomial of the LFSR is $\boxed{17}$.
  - The linear complexity of the sequence is $\boxed{18}$.

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

```
INPUT: a point $P$ on the curve, a positive integer $k = (k_{t-1}, ..., k_1, k_0)_2$
OUTPUT: the point $kP$ on the curve
1.  $R \leftarrow \infty$   ($O$: point at infinity)
2.  For  $i$  from  $t-1$  downto  0  do
        2.1  $R \leftarrow \boxed{19}$
        2.2  If  $k_i = 1$  then  $R \leftarrow \boxed{20}$
3.  Return ($R$)
```

- In the 2nd homework, you are asked to find a point of prime order in an elliptic curve (EC) group. Such a base point generating a cyclic group is a part of domain parameters of an elliptic curve cryptosystem (ECC). This set of problems will show you that if the order of the base point is not prime, then the discrete logarithm problem (DLP) on the EC group can be reduced to easier ones by the Pohlig-Hellman Attack. Let's solve the DLP $Q = xP$ where P is a base point on the EC group indicated by the figure.



   - ♦ Note that the order of the EC group is 30 = 2 × 3 × 5. We have $6P = (16, 14)$, $10P = (1, 2)$, $15P = (8, 0)$, $2Q = (9, 9)$, $4Q = \boxed{21}$, $6Q = (16, 9)$, $10Q = \boxed{22}$, $15Q = 16Q - Q = \boxed{23}$.
   - ♦ First, solve the DLP $(30/5)Q = 6Q = x(6P)$. Note that both $6P$ and $6Q$ lie in the subgroup of order 5. Writing $x = 5k_5 + x_5$ where $x_5 \in \mathbf{Z}_5$, we find $x_5 = 4$ since $6Q = 24P$, hence $x \equiv 4 \pmod 5$.
   - ♦ Second, solve the DLP $(30/3)Q = 10Q = x(10P)$. Note that both $10P$ and $10Q$ lie in the subgroup of order 3. Writing $x = 3k_3 + x_3$ where $x_3 \in \mathbf{Z}_3$, we find x_3, hence $x \equiv \boxed{24} \pmod 3$.
   - ♦ Third, solve the DLP $(30/2)Q = 15Q = x(15P)$. Note that both $15P$ and $15Q$ lie in the subgroup of order 2. Writing $x = 2k_2 + x_2$ where $x_2 \in \mathbf{Z}_2$, we find x_2, hence $x \equiv \boxed{25} \pmod 2$.
   - ♦ Combining the results by Chinese Remainder Theorem, we obtain $x = \boxed{26}$.

- Using Diffie-Hellman key exchange scheme on $\boldsymbol{Z}_{37}$ with the generator $g = 2$, Alice chooses 17 and Bob chooses 11 in private.
  - ♦ The element in $\boldsymbol{Z}_{37}$ that Alice sends to Bob is $\boxed{\textbf{27}}$.
  - ♦ The agreed key is $\boxed{\textbf{28}}$.

- If a random number generator (RNG) is not good enough, the public moduli of RSA generated by such RNG might be factored with a chance much higher than expected. A paper published in February 2012 claimed that 0.2% of millions of RSA moduli collected on the internet can be factored without knowing private keys. Suppose $n_1 = 9397331$ and $n_2 = 9794783$ with an unfortunate common prime factor are generated by a lousy RNG, then both moduli are factored easily. Assume $p > q$ are the prime factors of n_1, then $p = \boxed{\textbf{29}}$ and $q = \boxed{\textbf{30}}$.

Part III (Write down all details of your work)

$\boxed{31}$ (5 points) Decrypt the ciphertext $c = 54$ encrypted by the Rabin public-key cryptosystem $c = m \times (m + 16) \pmod{437}$.

$\boxed{32}$ (5 points) Which finalist of SHA-3 competition did you introduce in the 2nd homework? Describe this hash function as detailed as possible.

Cryptography Final Exam 2012/06/19

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 Final Exam 2012/06/19

Solution

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

11	12	13	14	15
280	187	1	26	287
16	17	18	19	20
S^e	x^3+x^2+1	3	$2R$	$R + P$
21	22	23	24	25
(14, 6)	(1, 2)	(8, 0)	1	1
26	27	28	29	30
19	18	17	3121	3011

31

m = 123, 146, 275, 298