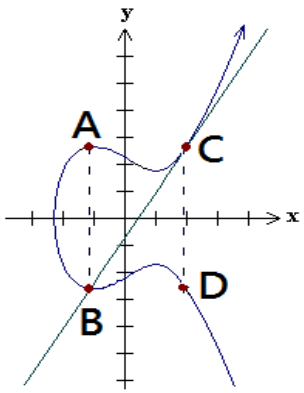
Cryptography Final Exam 2011/06/21

Part I (3 points each)

The right figure shows the graph of an elliptic curve over $\boldsymbol{R}$. The line BC is tangent to the curve at C. Both AB and CD are vertical lines. On the *elliptic curve group* denoted as an additive group, indicate the specified point on the figure in each of the following three questions.



E : Point at Infinity

1. Which point is $2C$?
2. Which point is $B + C$?
3. Which point is $B - 2D$?

4. Which equation does NOT define an elliptic curve group over GF_{23}?
   A. $y^2 = x^3 + 6x + 5$ B. $y^2 = x^3 + 7x + 5$
   C. $y^2 = x^3 + 8x + 5$ D. $y^2 = x^3 + 9x + 5$ 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 $(\boldsymbol{Z}_p^*, \times)$? Cryptographic primitives based on the discrete logarithm problem are operated on such groups.
   A. $p = 1831, q = 331$ B. $p = 1847, q = 317$
   C. $p = 1861, q = 313$ D. $p = 1867, q = 311$ E. None of the above

6. Whose security is NOT based on the difficulty of the *discrete logarithm problem*?
   A. ElGamal encryption B. Diffie-Hellman key exchange scheme
   C. Rabin encryption D. DSA (Digital Signature Algorithm) E. None of the above

7. Which is the first primality-proving algorithm to be simultaneously *polynomial*, *deterministic*, *general*, and *unconditional*?
   A. Fermat's test B. Miller-Rabin test
   C. ECPP test D. AKS test E. None of the above

8. *NSA Suite B* is a set of cryptographic algorithms promulgated by NSA (National Security Agency) of USA as part of its Cryptographic Modernization Program. Which algorithm is NOT included in NSA Suite B?
   A. RSA B. AES C. SHA-2 D. ECDH E. None of the above

9. Which statement is FALSE about Public Key Infrastructure?
   A. PKI provides the authentic channels used to distribute keys
   B. A digital certificate binds an entity and its public key
   C. Time stampings are signed by the public key of a trusted third party
   D. HTTP, FTP, TELNET protocols can be transparently layered on top of SSL
   E. None of the above

10. Which statement is FALSE about Identity Based Cryptography?
   A. Its first signature scheme is based on the RSA problem
   B. Its first encryption scheme is based on bilinear pairings on elliptic curves
   C. It removes the need for a trusted third party
   D. It removes the need for storage and transmission of certificates
   E. None of the above

Part II (3 points each)

- The RSA signature scheme applied with Chinese Remainder Theorem (CRT) is performed in many low-cost chips. Suppose $p = 17$ and $q = 23$ are kept private, and the public modulus is $n = 391 = 17 \times 23$.
  - The value of Euler ϕ-function for n is $\phi(391) =$ **11**.
  - If the public exponent for verification is $e = 3$, the corresponding private key for signing is $d =$ **12**, where $0 < d < \phi(391)$.
  - Sign the message $m = 124$ by CRT as follows.
    - $m^d \bmod p = (m \bmod p)^{d \bmod \phi(p)} \bmod p =$ **13** $= A$, where $0 \le A < p$.
    - $m^d \bmod q = (m \bmod q)^{d \bmod \phi(q)} \bmod q =$ **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 $S = m^d \bmod n =$ **15**, where $0 \le S < n$.
  - Verify the signature S as follows.
    - Compute $m' =$ **16** $\bmod n$. (Fill in a formula related to S and e)
    - If $m = m'$, then the digital signature S is accepted. Otherwise S is rejected.

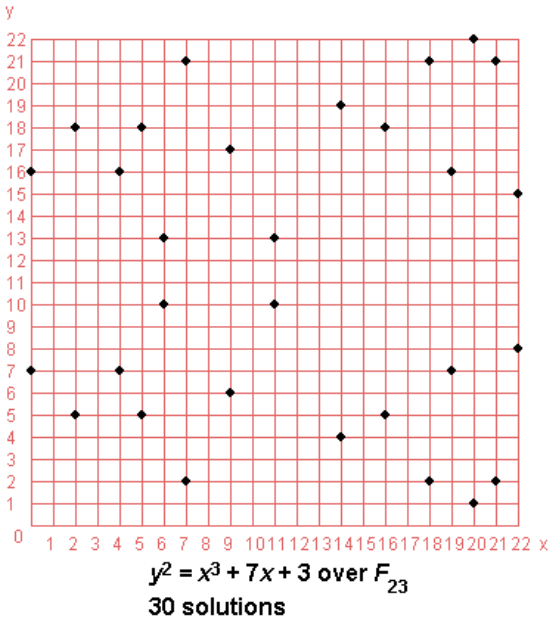
    Note that the correctness of your answers to the values of A, B, and S can be confirmed in a similar way.

- Alice and Bob will agree a key by the Diffie-Hellman key exchange scheme on $\boldsymbol{Z}_{53}$ with the generator $g = 2$. Evaluate the following values of A and K in $\boldsymbol{Z}_{53}$.
  - Alice selects $a = 21$ randomly in private, then Alice sends $A =$ **17** to Bob.
  - Bob selects $b = 8$ randomly in private and sends the corresponding B to Alice, then the agreed key is $K =$ **18**.

- $N = 79567 = p \times q$ has the value $\phi(N) = 79000$ of Euler ϕ-function. Assume the prime factors $p > q$, then $p =$ **19** and $q =$ **20**.

- $N = 43739 = p \times q$ satisfies:
$$296^2 \equiv 138 = 2 \times 3 \times 23 \pmod{N}$$
$$302^2 \equiv 3726 = 2 \times 3^4 \times 23 \pmod{N}$$
$$305^2 \equiv 5547 = 3 \times 43^2 \pmod{N}$$
$$363^2 \equiv 552 = 2^3 \times 3 \times 23 \pmod{N}$$
$$373^2 \equiv 7912 = 2^3 \times 23 \times 43 \pmod{N}$$
Assume the prime factors $p > q$, then $p =$ **21** and $q =$ **22**.

- Perform ECDSA on the elliptic curve group defined by $y^2 = x^3 + 7x + 3$ over $\boldsymbol{F}_{23}$ as the figure. The base point is $G = (7, 2)$.



  - The order of G is $n =$ **23**.
  - $2G =$ **24**.
  - Choose $x = 3$ randomly as the private key, then the public key is $P =$ **25**.
  - To sign a message m, the following steps are executed:
    - Calculate $e = \text{HASH}(m)$. Assume $z = 19$ is the L_n leftmost bits of e.
    - Choose $k = 5$ randomly as an ephemeral key.
    - Calculate $r = x_1 \bmod n$, where $(x_1, y_1) = kG =$ **26**.
    - Calculate $s = k^{-1}(z + rx) \bmod n =$ **27**.
    - The signature is the pair (r, s)
  - To verify the signature (r, s), the following steps are executed:
    - Calculate $t = z\,s^{-1} \bmod n$
    - Calculate $u = r\,s^{-1} \bmod n$
    - Calculate $v = x_2 \bmod n$, where $(x_2, y_2) = V = t\,G + u\,P$.
    - The signature (r, s) is accepted if **28**.

- This example demonstrates how to solve discrete logarithm problems by Shank's Baby-Step/Giant-Step algorithm. To solve $5^x \equiv 219 \pmod{307}$, write $x = i + 18k$ where $0 \le i, k < 18$. Note that 18 is the least integer greater than $\sqrt{307}$. List $(i, 5^i)$ and $(k, 219\times5^{-18k})$ by way of $5^{-18} \equiv 235 \pmod{307}$ as follows.

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

Determine i and k such that $5^i \equiv 219\times5^{-18k} \pmod{307}$ from the tables. We obtain $5^{i+18k} \equiv 219 \pmod{307}$ for $i =$ **29**. The solution is $x =$ **30** where $0 < x < 307$. Shank's Baby-Step/Giant-Step algorithm takes $O(\sqrt{n})$ space and $O(\sqrt{n})$ time to solve a discrete logarihm problem in a cyclic group of order n.

Part III (Write down all details of your work)

31 (5 points) Miller-Rabin Probabilistic Primality Test is recommended and specified in FIPS 186-3 and many other documents. It is widely implemented.
(a) Explain the concept behind the test.
(b) Describe its algorithm as precise as possible.

32 (5 points) Elliptic Curves over 256-bit and 384-bit prime fields are required by NSA Suite B for key agreements and digital signatures. The coefficients of the equation defining an elliptic curve must be selected carefully.
(a) Show that the polynomial $x^3 + ax + b$ has no repeated roots if and only if $4a^3 + 27b^2 \neq 0$.
(b) Why the equations $y^2 = x^3 + ax + b$ with $4a^3 + 27b^2 = 0$ must be avoided for ECC (Elliptic Curve Cryptography)?

Cryptography Final Exam 2011/06/21

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 2011/06/21

Solution

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

11	12	13	14	15
352	235	11	6	351
16	17	18	19	20
S^e	48	15	317	251
21	22	23	24	25
229	191	31	(2, 18)	(4, 16)
26	27	28	29	30
(18, 21)	27	$v = r$	4	130