Cryptography Final Exam 2010/06/22

Part I (3 points each)

1. Which is a *normal basis* of GF_{64} over GF_2 for a proper $t \in GF_{64}$?
A. $\{t, t^2, t^3, t^4, t^5, t^6\}$ B. $\{t, t^2, t^4, t^8, t^{16}, t^{32}\}$
C. $\{1, t, t^2, t^3, t^4, t^5\}$ D. $\{1, t, t^2, t^4, t^8, t^{16}\}$ E. None of the above

2. On the elliptic curve group defined by $y^2 = x^3 + ax + b$ over a prime field (GF_p), $R = (x_R, y_R)$ is the sum of $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. Which is x_R? (all modulo p)
A. $[(y_P - y_Q)/(x_P - x_Q)]^2 - x_P - x_Q$ B. $[(y_P + y_Q)/(x_P + x_Q)]^2 + x_P + x_Q$
C. $(y_P - y_Q)^2 - x_P - x_Q$ D. $(y_P + y_Q)^2 + x_P + x_Q$ E. None of the above

3. On the elliptic curve group defined by $y^2 + xy = x^3 + ax^2 + b$ over a binary field (GF_{2^m}), $-P$ is the inverse of $P = (x_P, y_P)$. Which is $-P$?
A. $(x_P, -y_P)$ B. $(-x_P, y_P)$ C. $(x_P, x_P + y_P)$ D. $(x_P + y_P, y_P)$ E. None of the above

4. Which is a public-key encryption scheme based on elliptic curves?
A. ECDH B. ECIES C. ECDSA D. ECMQV E. None of the above

5. Which is NOT a generator of a cyclic multiplicative group of order 11 in $\boldsymbol{Z}_{89}{}^*$?
A. $3^{(89-1)/11}$ B. $6^{(89-1)/11}$ C. $9^{(89-1)/11}$ D. $12^{(89-1)/11}$ E. None of the above

6. How many square roots of 1 in $\boldsymbol{Z}_{1155}$? i.e., the number of solutions to $x^2 \equiv 1 \pmod{1155}$?
A. 8 B. 12 C. 16 D. 20 E. None of the above

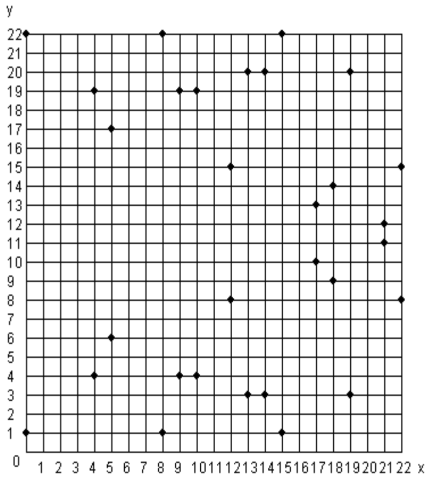
7. To generate a large prime, how many times at least should the Miller-Rabin test be repeated on a candidate integer to make sure the error probability $\leq 10^{-12}$?
A. 8 B. 12 C. 16 D. 20 E. None of the above

8. Which stream cipher is NOT in the portfolio of the eSTREAM project?
A. RC4 B. Trivium C. Salsa20 D. Rabbit E. None of the above

9. What is the fixed bit length of all outputs of the hash function SHA-1?
A. 128 B. 192 C. 256 D. 384 E. None of the above

10. Which should NOT be listed on a digital certificate? A. Private key
B. User name C. Expiry date D. Serial number E. None of the above

Part II (3 points each)



$y^2 = x^3 + 5x + 1$ over F_{23}
30 solutions

- Alice and Bob will agree a key by ECDH (Elliptic Curve Diffie-Hellman) on the group defined by $y^2 = x^3 + 5x + 1$ over GF_{23}. $G = (0, 1)$ is taken as the base point. Alice chooses $a = 27$ and sends $A = 27G = (22, 15)$ to Bob.
    - ♦ The order of the elliptic curve group is $\boxed{11}$.
    - ♦ $A + 4G = \boxed{12}$.
    - ♦ Bob chooses $b = 3$ and sends $B = \boxed{13}$ to Alice.
    - ♦ The agreed key comes from the x-coordinate of the point $nG = \boxed{14}$, where $n = \boxed{15}$.

- An RSA signature scheme is operated with the public modulus $n = 133 = 7 \times 19$.
    - ♦ $\varphi(133) = \boxed{16}$, the value of Euler φ-function for n.
    - ♦ If the public exponent for verification is $e = 5$, the corresponding private key for signing is $d = \boxed{17}$.
    - ♦ Signing the message $m = 3$, the user obtains its digital signature $s = \boxed{18}$.

- In Shamir's secret sharing scheme with threshold 3 over GF_{19}, the secret a_0 is hided as the constant of the polynomial $f(x) = a_2 x^2 + a_1 x + a_0 \in GF_{19}[x]$.
    - ♦ The points (1, 8), (3, 18), (5, 6) that $f(x)$ passes are obtained from three participants, then the secret is recovered as $a_0 = \boxed{19}$.
    - ♦ The point $(2, y)$ is also distributed to another participant, then $y = \boxed{20}$.

- Complete the signature generation algorithm of ECDSA (Elliptic Curve Digital Signature Algorithm). Note that domain parameters for ECDSA are of the form (q, FR, a, b, G, n, h), where q is the field size, FR is an indication of the basis used, a and b are two field elements that define the equation of the curve, G is a base point of prime order on the curve (i.e., $G = (x_G, y_G)$), n is the order of the point G, and h is the cofactor (which is equal to the order of the curve divided by n). Let L_n be the bit length of the group order n.
    - ♦ The private key d is a randomly selected integer in the interval $[1, n-1]$. The corresponding public key is a point P on the curve, where $P = \boxed{21}$.
    - ♦ To sign a message m, the following steps are executed:
        1. Calculate $e = \text{HASH}(m)$. Let z be the L_n leftmost bits of e.
        2. Select a random integer k from $[1, n-1]$.
        3. Calculate $r = x_1 \pmod{n}$, where $(x_1, y_1) = kG$. If $r = 0$, go back to step 2.
        4. Calculate $s = k^{-1}(\boxed{22}) \pmod{n}$. If $s = 0$, go back to step 2.
        5. The signature is the pair (r, s)

- From $12860^2 \equiv 5185^2$ (mod 123107), the prime factorization $123107 = p \times q$ is obtained as $p = \boxed{23}$ and $q = \boxed{24}$ with $p > q$.

- For a 32-bit machine and 64-bit numbers, $x = x_1 2^{32} + x_0$ and $y = y_1 2^{32} + y_0$ are multiplied by Karatsuba technique which requires 3 multiplications instead of 4.
    - Compute $A = x_1 \cdot y_1$, $B = x_0 \cdot y_0$, and $C = \boxed{25}$ (in terms of x_0, x_1, y_0, y_1).
    - Then $x \cdot y$ is given by $A 2^{64} + D 2^{32} + B$, where $D = \boxed{26}$ (in terms of A, B, C).

- The sequence 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, … is generated by an LFSR (linear feedback shift register) of linear complexity 4.
    - The period of the sequence is $\boxed{27}$.
    - The next three bits (11th ~ 13th bit) of the sequence are $\boxed{28}$.

- Complete the Left-to-Right binary exponentiation algorithm:
  INPUT: P and $k = (k_{t-1}, ..., k_1, k_0)_2$
  OUTPUT: P^k

```
1. $Q \leftarrow 1$
2. For $i$ from $t-1$ downto 0 do
    2.1 $Q \leftarrow \boxed{29}$
    2.2 If $k_i = 1$ then $Q \leftarrow \boxed{30}$
3. Return ($Q$)
```

Part III (Write down all details of your work)

$\boxed{31}$ (3 points) Let $n = 6601$. Show that $a^n \equiv a$ (mod n) for every integer a, i.e., 6601 is a Carmichael number. Hint: Chinese Remainder Theorem.

$\boxed{32}$ (7 points) **NSA Suite B** is a set of cryptographic algorithms promulgated by *National Security Agency* as part of its Cryptographic Modernization Program.

- Describe the components of Suite B for the usage of (1) symmetric encryption, (2) digital signature, (3) key agreement, and (4) message digest, respectively.

- Specify these algorithms with key size, output size, or base field size, such that they are sufficient for protecting classified information up to the **Secret** level.

- Specify these algorithms with key size, output size, or base field size, such that they are necessary for the protection of **Top Secret** information.

Cryptography Final Exam 2010/06/22

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 2010/06/22

Solution

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

11	12	13	14	15
31	O (point at infinity)	(13, 3)	(17, 13)	19 (or 81)
16	17	18	19	20
108	65	124	9	11
21	22	23	24	25
dG	$z+rd$	401	307	$(x_1+x_0)(y_1+y_0)$
26	27	28	29	30
$C-A-B$	15	1,1,0	Q^2	$Q\times P$

31 Hint: 6601 = 7 × 23 × 41. Verify the congruence modulo 7, 23, 41 respectively by Fermat little theorem or Euler theorem, then apply CRT.

32 (1) AES (with 128/256-bit keys, and Galois Counter Mode [GCM])
(2) ECDSA (elliptic curves over 256/384-bit prime fields)
(3) ECDH (elliptic curves over 256/384-bit prime fields)
(4) SHA-2 (256/384-bit outputs)
Secret: AES-128, SHA-256, 256-bit EC
Top Secret: AES-256, SHA-384, 384-bit EC