Cryptography Exam 3 2012/11/20

Part I (3 points each)

1. For which of the following n, the square matrix $\begin{bmatrix} 1 & 2 & 4 \\ 4 & 3 & 6 \\ 5 & 4 & 2 \end{bmatrix}$ is invertible over $\boldsymbol{Z}_n$?
   A. 2010 B. 2011 C. 2012 D. 2013 E. None of the above

2. How many *irreducible* polynomials of degree 5 over GF_2?
   A. 6 B. 8 C. 10 D. 12 E. None of the above

3. Apply Fermat's primality test on 21. Which is NOT a *witness of compositeness*?
   A. 2 B. 4 C. 8 D. 16 E. None of the above

4. 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 $\leq 10^{-15}$?
   A. 15 B. 20 C. 25 D. 30 E. None of the above

5. Whose operation of S-box is speeded up by the *bitslice* technique?
   A. Serpent B. SMS4 C. IDEA D. AES E. None of the above

6. Which hash function was announced to win the SHA-3 competition?
   A. BLAKE B. Grøstl C. JH D. Skein E. None of the above

7. Which construction is SHA-3 based on?
   A. Feistel B. Substitution-permutation network
   C. Sponge D. Merkle-Damgård E. None of the above

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

9. Which is NOT one of the operations of the IDEA encryption?
   A. Multiplication modulo $2^{16}+1$ B. Exponentiation modulo $2^{16}-1$
   C. Addition modulo 2^{16} D. Exclusive OR E. None of the above

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

Part II (3 points each)

- Select appropriate mode(s) of operation with specified property respectively from the following list: A. ECB B. CBC C. OFB D. CFB E. CTR F. CCM G. GCM H. XEX I. XTS-AES J. CBC-CS1
  - Use multiplications in the Galois field $GF_{2^{128}}$: $\boxed{11}$
  - Generate *periodic* key stream with fixed key and IV: $\boxed{12}$
  - Decryption can be parallelized while encryption can *not* be parallelized: $\boxed{13}$
  - Designed for confidentiality on storage devices: $\boxed{14}$
  - Use the technique of *ciphertext stealing*: $\boxed{15}$
  - Authenticated encryption: $\boxed{16}$

- 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, 6), (2, 4), (4, 12) that $f(x)$ passes are obtained from three participants, then the secret is recovered as $a_0 = \boxed{17}$.
  - The point $(3, y)$ is also distributed to another participant, then $y = \boxed{18}$.

- On a 64-bit machine, two 128-bit numbers, $x = x_1 2^{64} + x_0$ and $y = y_1 2^{64} + y_0$, are multiplied with Karatsuba technique which requires 3 multiplications instead of 4.
  - Compute $A = x_1 \cdot y_1$, $B = x_0 \cdot y_0$, and $C = \boxed{19}$ (in terms of x_0, x_1, y_0, y_1).
  - Then $x \cdot y$ is given by $A\,2^{128} + D\,2^{64} + B$, where $D = \boxed{20}$ (in terms of A, B, C).

Part III (Write down all details of your work)

$\boxed{21}$ (4 points) Show that a group G is *abelian* if $a^2 = e$ for all $a \in G$.

$\boxed{22}$ (6 points) Find all possible n such that $\varphi(n) = 16$.

$\boxed{23}$ (6 points) Solve $x^2 + 7x + 1 \equiv 0 \pmod{45}$ by Chinese Remainder Theorem.

$\boxed{24}$ (6 points) Explain the technique of *ciphertext stealing* used in some modes of operation. What advantage does it have?

$\boxed{25}$ (6 points) Explain *Montgomery reduction* for modular arithmetic. What advantage does it have?

$\boxed{26}$ (12 points) Factor $n = 3837523$ by Quadratic Sieve as below.

	2	3	5	7	11	13	17	19
1964^2	0	2	0	0	0	3	0	0
3397^2	5	0	1	0	0	2	0	0
8077^2	1	0	0	0	0	0	0	1
9398^2	0	0	5	0	0	0	0	1
14262^2	0	0	2	2	0	1	0	0
17078^2	6	2	0	0	1	0	0	0
19095^2	2	0	1	0	1	1	0	1

The second row means $1964^2 \equiv 3^2 \times 13^3 \pmod{n}$.

(a) Find $a_1, a_2, \ldots, a_k$ such that $(a_1, a_2, \ldots, a_k)^2$ mod n is a square on the given factor base

(b) Find a and b such that $a^2 \equiv b^2 \pmod{n}$

(c) Factor n

Cryptography Exam 3 2012/11/20

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 ~ 26

Cryptography Exam 3 2012/11/20

Solution

1	2	3	4	5	6	7	8	9	10
B	A	C	C	A	E	C	D	B	A
11		12		13		14		15	
G H I		C (E F G)		B D J		H I		I J	
16		17		18		19		20	
F G		12		6		$(x_1+x_0)(y_1+y_0)$		$C-A-B$	

22 17, 32, 34, 40, 48, 60

23 4, 19, 34 (mod 45)

26 1093 × 3511