Cryptography Final Exam 2009/06/16

Part I (3 points each)

1. Apply Fermat's primality test on 33. Which is NOT a *witness of compositeness*?
   A. 7 B. 10 C. 13 D. 16 E. None of the above

2. Which is the key length (in bits) of *two-key* Triple-DES?
   A. 112 B. 128 C. 160 D. 192 E. None of the above

3. The S-box of AES is constructed by combining the function $f(x) = x^a$ defined on GF_{256} with an invertible affine transformation. Which is the value of a?
   A. 254 B. 255 C. 256 D. 257 E. None of the above

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

5. Which mode of operation has no error propagation? That is, a transmission error of one bit causes a decryption error of only one bit.
   A. ECB B. CBC C. OFB D. CFB E. None of the above

6. Suite B is a set of algorithms promulgated by National Security Agency (NSA) as part of Cryptographic Modernization Program. Which is NOT included in Suite B?
   A. ECDH B. ECDSA C. AES-256 D.SHA-256 E. None of the above

7. Let m_i's and c_i's be plaintext and ciphertext blocks respectively. With a decryption algorithm d and a key k, which is the decryption operation of CBC mode for $i > 1$?
   A. $m_i = d_k(c_i \oplus m_{i-1})$ B. $m_i = d_k(c_i) \oplus m_{i-1}$
   C. $m_i = d_k(c_i \oplus c_{i-1})$ D. $m_i = d_k(c_i) \oplus c_{i-1}$ E. None of the above

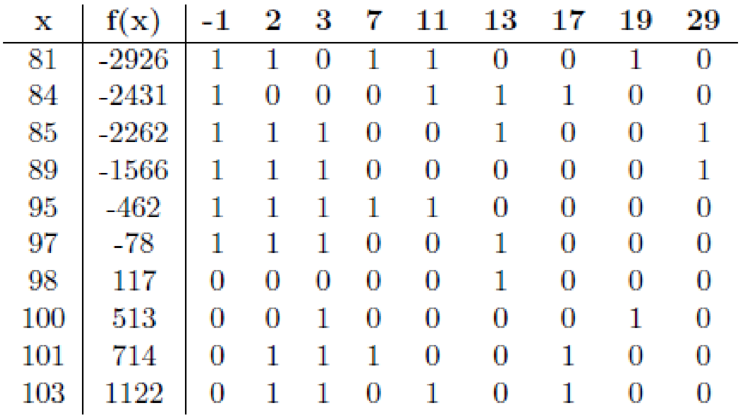
8. Which signature scheme based on discrete logarithm problem has the *message recovery* property? A. ElGamal signature B. DSA
   C. Nyberg-Rueppel signature D. Schnorr signature E. None of the above

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

10. Which statement is FALSE about PKI?
    A. CRL is a list of the serial numbers of all the revoked certificates
    B. CA establishes the identity of users, but does not sign certificates
    C. SSL aims to provide channel security to fulfill commercial requirement
    D. X509 defines a structure for public key certificates
    E. None of the above

Part II (3 points each)

- To factor 9487 by the quadratic sieve, we define $f(x) = x^2 - 9487$.



x	f(x)	-1	2	3	7	11	13	17	19	29
81	-2926	1	1	0	1	1	0	0	1	0
84	-2431	1	0	0	0	1	1	1	0	0
85	-2262	1	1	1	0	0	1	0	0	1
89	-1566	1	1	1	0	0	0	0	0	1
95	-462	1	1	1	1	1	0	0	0	0
97	-78	1	1	1	0	0	1	0	0	0
98	117	0	0	0	0	0	1	0	0	0
100	513	0	0	1	0	0	0	0	1	0
101	714	0	1	1	1	0	0	1	0	0
103	1122	0	1	1	0	1	0	1	0	0

Note that $513 = 3^3 \times 19$.

    - ♦ From the table, $(81 \times \boxed{11} \times \boxed{12})^2 \equiv a^2 \pmod{9487}$ where a is an integer.
    - ♦ The factorization is $9487 = \boxed{13} \times \boxed{14}$.

- DES and Triple-DES support the data block size of $\boxed{15}$ bits. AES supports the data block size of $\boxed{16}$ bits.

- A cryptographic hash function h should satisfy the following properties.
    - ♦ Pre-image Resistance: Given y, hard to find x such that $\boxed{17}$.
    - ♦ Collision Resistance: Hard to find any $x \neq x'$ such that $\boxed{18}$.

- Consider the sequences generated by an LFSR with register length 6.
    - ♦ The largest possible period of a sequence is $\boxed{19}$.
    - ♦ With the connection polynomial $x^6 + x^3 + 1$, the period of a non-zero sequence is $\boxed{20}$.

- Using Diffie-Hellman key exchange scheme on $\mathbf{Z}_{37}$ with the generator $g = 2$, Alice chooses 12 and Bob chooses 5 in private.
    - ♦ The element in $\mathbf{Z}_{37}$ that Alice sends to Bob is $\boxed{21}$.
    - ♦ The agreed key is $\boxed{22}$.

- The following reference code comes from the book “The Design of Rijndael” written by J. Daemen and V. Rijmen:

```
typedef unsigned char word8;

word8 Logtable[256] = {
  0,  0, 25,  1, 50,  2, 26,198, 75,199, 27,104, 51,238,223,  3,100,  4,224, 14,
 52,141,129,239, 76,113,  8,200,248,105, 28,193,125,194, 29,181,249,185, 39,106,
 77,228,166,114,154,201,  9,120,101, 47,138,  5, 33, 15,225, 36, 18,240,130, 69,
 53,147,218,142,150,143,219,189, 54,208,206,148, 19, 92,210,241, 64, 70,131, 56,
102,221,253, 48,191,  6,139, 98,179, 37,226,152, 34,136,145, 16,126,110, 72,195,
163,182, 30, 66, 58,107, 40, 84,250,133, 61,186, 43,121, 10, 21,155,159, 94,202,
 78,212,172,229,243,115,167, 87,175, 88,168, 80,244,234,214,116, 79,174,233,213,
231,230,173,232, 44,215,117,122,235, 22, 11,245, 89,203, 95,176,156,169, 81,160,
127, 12,246,111, 23,196, 73,236,216, 67, 31, 45,164,118,123,183,204,187, 62, 90,
251, 96,177,134, 59, 82,161,108,170, 85, 41,157,151,178,135,144, 97,190,220,252,
188,149,207,205, 55, 63, 91,209, 83, 57,132, 60, 65,162,109, 71, 20, 42,158, 93,
 86,242,211,171, 68, 17,146,217, 35, 32, 46,137,180,124,184, 38,119,153,227,165,
103, 74,237,222,197, 49,254, 24, 13, 99,140,128,192,247,112,  7};

word8 Alogtable[256] = {
  1,  3,  5, 15, 17, 51, 85,255, 26, 46,114,150,161,248, 19, 53, 95,225, 56, 72,
216,115,149,164,247,  2,  6, 10, 30, 34,102,170,229, 52, 92,228, 55, 89,235, 38,
106,190,217,112,144,171,230, 49, 83,245,  4, 12, 20, 60, 68,204, 79,209,104,184,
211,110,178,205, 76,212,103,169,224, 59, 77,215, 98,166,241,  8, 24, 40,120,136,
131,158,185,208,107,189,220,127,129,152,179,206, 73,219,118,154,181,196, 87,249,
 16, 48, 80,240, 11, 29, 39,105,187,214, 97,163,254, 25, 43,125,135,146,173,236,
 47,113,147,174,233, 32, 96,160,251, 22, 58, 78,210,109,183,194, 93,231, 50, 86,
250, 21, 63, 65,195, 94,226, 61, 71,201, 64,192, 91,237, 44,116,156,191,218,117,
159,186,213,100,172,239, 42,126,130,157,188,223,122,142,137,128,155,182,193, 88,
232, 35,101,175,234, 37,111,177,200, 67,197, 84,252, 31, 33, 99,165,244,  7,  9,
 27, 45,119,153,176,203, 70,202, 69,207, 74,222,121,139,134,145,168,227, 62, 66,
198, 81,243, 14, 18, 54, 90,238, 41,123,141,140,143,138,133,148,167,242, 13, 23,
 57, 75,221,124,132,151,162,253, 28, 36,108,180,199, 82,246,  1};

/* The tables Logtable and Alogtable are used to perform multiplications in GF(256)

word8 mul(word8 a, word8 b) {
  if (a && b) return Alogtable[(Logtable[a] + Logtable[b])%255];
  else return 0;
}
```

GF_{256} is generated by $m(x) = x^8 + x^4 + x^3 + x + 1$ in AES. The above tables (20 entries in each row) are built by the primitive element $x+1$ of $GF_2[x]/<m(x)> \cong GF_{256}$.

- $(x+1)^n \bmod m(x) = x^4 + x$, then $n = \boxed{23}$.
- $(x+1)^{179} \bmod m(x) = \boxed{24}$ (a polynomial in $GF_2[x]$ of degree < 8)
- $(x^5+x^2)^{-1} \bmod m(x) = \boxed{25}$ (a polynomial in $GF_2[x]$ of degree < 8)
- Finish the subroutine computing patched multiplicative inverses in GF_{256}:

```
word8  inverse(word8 a) {
  if (a) return Alogtable[ 26 ];
  else return 0;
}
```

- Consider Shamir's Secret Sharing with threshold 3 over GF_{17}. The secret a_0 is hided as the constant of the polynomial $f(x) = a_2x^2 + a_1x + a_0 \in GF_{17}[x]$.
  - The points (1, 6), (2, 10), (4, 2) that $f(x)$ passes are obtained from three participants. Then the secret is recovered as $a_0 = \boxed{27}$.
  - The point $(3, y)$ is also distributed to another participant, then $y = \boxed{28}$.

- Complete the Miller-Rabin test to determine the primality of an integer n:

```
Write   $n-1 = 2^k m$   where $m$ is odd
Choose   $a \in \{1, \ldots, n-1\}$
Compute   $b = \boxed{29}$   (mod $n$)
If   $(b \neq 1$ and $b \neq (n-1))$
    $i = 1$
    While   $(i < k$  and  $b \neq (n-1))$
        $b = \boxed{30}$   (mod $n$)
        If   $(b = 1)$   Output (Composite, $a$)
        $i = i + 1$
    If   $(b \neq (n-1))$   Output (Composite, $a$)
Output "Probable Prime"
```

Part III (Write down all details of your work)

$\boxed{31}$ (4 points)

Both 1009 and 10091 are prime numbers. Find an element of the multiplicative group $\boldsymbol{Z}_{10091}^*$ whose order is 1009. Explain why your choice is correct. (Hint: The domain parameter selections of DLP-based cryptosystems such as DSA and ElGamal have similar process.)

$\boxed{32}$ (6 points)

In the MixColumns operation of AES, each column is treated as a polynomial over GF_{256} and is then multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = c_3x^3 + c_2x^2 + c_1x + c_0$. In AES, $c(x) = \text{'03'}x^3 + \text{'01'}x^2 + \text{'01'}x + \text{'02'}$ is selected specifically. This step can also be viewed as a multiplication by a particular matrix, $\boldsymbol{b} = C\boldsymbol{a}$ over GF_{256}:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

(a) A polynomial $c(x)$ is called *self-invertible* if $c(x)^2 \equiv 1$ (mod $x^4 + 1$). Show that $c(x)$ is self-invertible if and only if $c(x)$ is of the form $u\,x^3 + v\,x^2 + u\,x + (v + 1)$, where u and v are arbitrary elements in GF_{256}.

(b) The diffusion effect of the operation is evaluated by the *branch number*:

$$\min_{\boldsymbol{a} \neq 0} (W(\boldsymbol{a}) + W(C\boldsymbol{a}))$$

where $\boldsymbol{a}$ is a 4-byte vector, C is the matrix multiplier, W is the weight of a vector (the number of non-zero entries). Show that the maximal branch number is 5.

Remark: $c(x)$ = '03'x^3 + '01'x^2 + '01'x + '02' in AES has branch number 5.

(c) Show that the branch number of every self-invertible polynomial is less than or equal to 4.

Cryptography Final Exam 2009/06/16

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 2009/06/16

Solution

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

11	12	13	14	15
95	100	53	179	64

16	17	18	19	20
128	$y = h(x)$	$h(x) = h(x')$	63	9

21	22	23	24	25
26	10	224	$x^6 + x^4 + x^3$	$x^6+x^4+x^2+1$

26	27	28	29	30
255 – Logtable[a]	8	3	a^m	b^2

31 $g = 2^{(10091-1)/1009} = 2^{10} = 1024$,

$g^{1009} = 1 \pmod{10091}$ by the Little Fermat Theorem

32 (c) $\min_{\boldsymbol{a}\neq 0}(W(\boldsymbol{a}) + W(C\boldsymbol{a})) \le 2 + 2 = 4$, since

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} u+v+1 & u & u+v & u \\ u & u+v+1 & u & u+v \\ u+v & u & u+v+1 & u \\ u & u+v & u & u+v+1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$