Cryptography Midterm Exam 2012/05/01

Part I (3 points each)

1. Which multiplicative group is NOT cyclic?

A. ***Z***9\* B. ***Z***10\* C. ***Z***11\* D. ***Z***12\* E. None of the above

2. Which can NOT be the number of elements of a Galois field?

A. 100 B. 101 C. 121 D. 125 E. None of the above

3. Which is NOT a legitimate key length (in bits) of AES?

A. 128 B. 160 C. 192 D. 256 E. None of the above

4. Which of the following is a public-key cryptosystem?

A.RSA B. DES C. AES D.Caesar cipher E. None of the above

5. For a ring homomorphism *f* : *GF* 2[ *x*]*/* < *x*3+*x*2+1 > → *GF* 2[ *x*]*/* < *x*3+*x*+1 > between two quotient rings (*GF* 8), which assignment of*f*(*x*) makes*f*an *isomorphism*?

A. *f*(*x*)=*x* B. *f*(*x*)=*x*2  C. *f*(*x*)=*x*+1 D. *f*(*x*)=*x*2+*x* E. None of the above

6. Except “Key Addition”, what is the correct order of operations in a typical round of AES encryption? (P) MixColumn (Q) SubByte (R) ShiftRow

A. RPQB. RQP C. QPRD. PRQ E. None of the above

7. Which quotient ring is NOT isomorphic to *GF* 32?

A. *GF* 2 [ *x*] */* <*x*5+*x*2 +1 > B. *GF* 2 [ *x*] */* <*x*5+*x*4 +*x*2+*x*+1 >

C. *GF* 2 [ *x*] */* <*x*5+*x* +1 > D. *GF* 2 [ *x*] */* <*x*5+*x*3 +*x*2+*x*+1 > E. None of the above

8. Which of the following is true?

A. There are exactly  primitive polynomials of degree 2012 over *GF*2

B. There are exactly 22012 −1 generators of (, ×)

C. There are exactly 22012 roots of  in

D. There are exactly 2012 subfields in

E. None of the above.

9. Which description is true for *GF*9[*x*]?

A. A ring but not a commutative ring

B. A commutative ring but not an integral domain

C. An integral domain but not a principle ideal domain

D. A principle ideal domain but not a field

E. A field

10. Which statement is true for historical ciphers? (To avoid possible confusion,

a *polyalphabetic substitution cipher* is not considered as a substitution cipher)

A. A Vigenère cipher is a special case of substitution ciphers

B. A Substitution cipher is a special case of Hill ciphers

C. A Hill cipher is a special case of permutation ciphers

D. A permutation cipher is a special case of Vigenère ciphers

E. None of the above

Part II (3 points each)

* *x* ≡ **11** (mod **12** ) is the solution to the system of congruences

*x* ≡ 5 (mod 9) *x* ≡ 2 (mod 8) *x* ≡ 4 (mod 7)

* *a* = **13** and*b* = **14** is the pair of integers satisfying56*a* + 71*b* = 1 where *a*is the least positive one. The solution to the equation56*x* ≡ 4 (mod 71)is *x* ≡ **15** (between 0 and 71).
* Euler’s Theorem and Fermat Little Theorem
* The least positive integer *m*satisfying*a m* ≡ 1 (mod 2011)for all*a*relatively prime to 2011 is*m* = **16**
* 22012 mod 41 = **17** (between 0 and 41)
* 22012 mod 42 = **18** (between 0 and 42)

|  |  |  |
| --- | --- | --- |
| Block cipher | DES / 3DES | AES |
| Block size (bits) | **19** | **20** |

* Complete the table:



* Applying the secret permutation on the plaintext CRYPTO,

we obtain the ciphertext PTYCOR. Suppose the permutation *σ* is applied



on CRYPTO to obtain OCTPRY, then*σ* 2 = **21** and*σ* −1 = **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 constructed 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*+1of*GF*2 [ *x*]*/*<*m*(*x*)> ≅ *GF*256.

* To show that *x*+1 is a primitive element of *GF*2 [ *x*]*/*<*m*(*x*)>, it is sufficient to verity that(*x*+1)*u* ≠ 1, (*x*+1)*v* ≠ 1, and (*x*+1)*w* ≠ 1. If1 < *u* < *v* < *w* < 256, then*v* = **23** and*w* = **24**.
* If*x*8+*x*4+*g*(*x*)­is a primitive polynomial over *GF*2, then the degree-3 polynomial *g*(*x*) = **25**
* Express the elements of *GF*256 in hexadecimal as AES does, then

‘8A’ + ‘5F’ = **26**, ‘8A’ × ‘5F’ = **27**,

(‘8A’)100 = **28**, (‘5F’)−1 = **29** (all in hexadecimal)

* Finish the subroutine computing patched multiplicative inverses in *GF*256:

word8 inverse(word8 a) {

if (a) return Alogtable[ **30** ];

else return 0;

}

Part III (Write down all details of your work)

31 (3 points) Prove that the identity element*e*in a group*G*is unique.

32 (7 points)

1. Find the minimal number *A* >1, such that*A*is NOT the order of a finite field.
2. Find the minimal number *B* >1, such that 4*B* is NOT the order of the

multiplicative group (, ×) for any integer *n.*Cryptography Midterm Exam 2012/05/01

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 Midterm Exam 2012/05/01

Solution

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| D | A | B | A | C | E | C | A | D | E |
| 11 | | 12 | | 13 | | 14 | | 15 | |
| 410 | | 504 | | 52 | | −41 | | 66 | |
| 16 | | 17 | | 18 | | 19 | | 20 | |
| 2010 | | 37 | | 4 | | 64 | | 128 | |
| 21 | | 22 | | 23 | | 24 | | 25 | |
| (15623) | | (16352) | | 51 | | 85 | | *x*3 +*x*2+1 | |
| 26 | | 27 | | 28 | | 29 | | 30 | |
| D5 | | 24 | | 9A | | 17 | | 255 −  Logtable[*a*] | |

31

32 *A* = 6, *B* = 17