Cryptography Midterm Exam 2011/04/19

Part I (3 points each)

1. Which multiplicative group is isomorphic to (***Z***5\*, ×)?

A. (***Z***8\*, ×) B. (***Z***10\*, ×) C. (***Z***12\*, ×) D. (***Z***15\*, ×) E. None of the above

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

A. 97 B. 64 C. 49 D. 36 E. None of the above

3. Which ideal is NOT the same as the principal ideal< 6 >in *Z*?

A.<−6> B.<18,−24>C.<36,48>D.<60,72,−30> E. None of the above

4. Which is a generator (primitive element) of the multiplicative group *Z* 41\*?

A. 2 B. 3 C. 4 D. 5 E. None of the above

5. An S-box is denoted by “*m*×*n*” if its inputs and outputs are *m*-bit and *n*-bit long respectively. How to denote the S-boxes of DES?

A. 8×8 B. 4×4 C. 8×6 D. 6×4 E. None of the above

6. Which quotient ring is isomorphic to *GF* 125?

A. *GF* 5 [ *x*] */* <*x*3+2*x* +1 > B. *GF* 5 [ *x*] */* <*x*3+*x*2+3 >

C. *GF* 5 [ *x*] */* <*x*3+2*x* +2 > D. *GF* 5 [ *x*] */* <*x*3+*x*2+4 > E. None of the above

7. Which is the best description of the Caesar Cipher?

A. Hill Cipher B. Substitution Cipher

C. Shift Cipher D. Permutation Cipher E. None of the above

8. Without which operation, AES becomes a cipher operating on four independent 32-bit blocks, that is, 1-bit change in plaintext affects 32-bit range in ciphertext?

A. ByteSub B. ShiftRow

C. MixColumn D. KeyAddition E. None of the above

9. Which statement is true for AES?

A. The S-box for ByteSub operation is also used in the key schedule

B. Designed by Joan Daemen and Vincent Rijmen of IBM, USA

C. Constructed as the structure of Feistel cipher

D. Some operations are performed in the Galois Field *GF* 128

E. None of the above

10. Which statement is true for block cipher modes of operation?

A. ECB needs initialization vectors (IV)

B. CBC ciphertext depends on all previous blocks

C. OFB keystream is generated by encrypting ciphertext

D. CFB has no ciphertext error propagation

E. None of the above

Part II (3 points each)

* *a* = **11** and*b* = **12** is the pair of integers satisfying61*a* + 43*b* = 1 with the condition that *a* is the least positive one.
* In the multiplicative group (***Z***61\*, ×):
* 43−1 (the multiplicative inverse of 43) = **13**.
* *o*(9) (the order of 9) = **14**.
* To prove that 2 is a generator of the group, it is sufficient to show that2*u* ≠ 1, 2*v* ≠ 1, and 2*w* ≠ 1. If1 < *u* < *v* < *w* < 61, then*v* = **15** and*w* = **16**.
* *x* ≡ **17** (mod **18** ) is the solution to the equation396*x* ≡ 308 (mod 968)
* A subset*H*of a group (*G*, \*) is a subgroup of*G*if and only if
* **19**∈ *H*for all*a*, *b* ∈ *H*; and
* **20**∈ *H*for all*a* ∈ *H.*
* Galois field*GF*64 is unique up to isomorphism.
* *GF*64 consists of all roots of*f*(*x*) = **21** of degree 64 over*GF*2.
* Represent*GF*64 by the quotient ring*K = GF*2 [*x*] */* < *x*6+*x*5+ *x*3+*g*(*x*) >, then

*g*(*x*) = **22**  of degree 2 over*GF*2.

* *h*(*x*)is a polynomial of degree ≤ 5 over*GF*2 satisfying the relation of cosets[*x*2011]=[*h*(*x*)]in*K*, then*h*(*x*) = **23**. [Hint: Reducing the exponent to an integer (could be negative) with a small absolute value might reduce the computation significantly]
* Clarify the potential of parallel processing for the following modes of operation:

(A) ECB (B) CBC (C) OFB (D) CFB

The cipher operations can be performed in parallel if the input block to each cipher does not depend on the result of the previous cipher operation.

* In the encryption of **24**, ciphers can be computed in parallel if plaintext blocks are immediately available.
* In the decryption of **25**, ciphers can be computed in parallel if ciphertext blocks are immediately available.

[Note: Fill in A, B, C, or D. There might be two or more to fill in one blank.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Block cipher | DES | AES | | |
| Block size (bits) | **26** | 128 | | |
| Key size (bits) | 56 | **27** | 192 | 256 |
| Number of rounds | 16 | **28** | 12 | 14 |

* Complete the table:
* The S-box of AES is constructed as follows.

*ai,j*-1

*bi,j*

* *ai,j* → *ai,j*-1→ *bi,j*



* *ai,j* ×*ai,j*-1 *=* 1(mod *x*8+*x*4+*x*3+*x*+1) but 0-1*=*0
* Affine transformation: *ai,j*-1→ *bi,j*
* Complete the last mapping in hexadecimal:
  + - 00→00→63[= (01100011)2]
    - 01→01→7C[= (01111100)2]
    - 0F→ **29**→ **30**

Part III (Write down all details of your work)

31 (3 points) Prove that the inverse of any element*g*in a group*G*is unique.

32 (3 points) To show that the Galois field*GF*8 is unique up to isomorphism, construct an isomorphism between the quotient rings

*R*1 *= GF*2[*x*] */* < *x*3+*x*2 +1> and *R*2 *= GF*2[*x*] */* < *x*3+*x*+1>.

That is, determine*h*(*x*)∈*GF*2[*x*]such that the homomorphism*f* : *R*1 → *R*2 defined by*f*([0]) = [0],*f*([1]) = [1], and*f*([*x*]) = [*h*(*x*)]is one-to-one and onto, where [*t*] denotes the coset that*t*belongs to. Explain why your choice is correct.

33 (4 points) Every input column and output column of the MixColumn operation of AES is treated as and over *GF*256 respectively. A fixed polynomial is selected in advance to perform the MixColumn transformation over*GF*256. Derive the assignments of*bi*’sin terms of*ai*’sand*ci*’sin matrix form. That is, find a 4×4 matrix *M*such that .

Cryptography Midterm Exam 2011/04/19

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 ~ 33

Cryptography Midterm Exam 2011/04/19

Solution

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| B | D | C | E | D | A | C | B | A | B |
| 11 | | 12 | | 13 | | 14 | | 15 | |
| 12 | | −17 | | 44 | | 5 | | 20 | |
| 16 | | 17 | | 18 | | 19 | | 20 | |
| 30 | | 13 | | 22 | | *a* \* *b* | | *a* −1 | |
| 21 | | 22 | | 23 | | 24 | | 25 | |
| *x*64− *x* | | *x*2+1 | | *x*5+ *x*+1 | | A | | ABD | |
| 26 | | 27 | | 28 | | 29 | | 30 | |
| 64 | | 128 | | 10 | | C7 | | 76 | |

31

32 *h*(*x*) = *x*+1, *x*2+*x*+1, or *x*2+1

33