

1. Find the determinant and the multiplicative inverse of the following residue matrix

A over  $Z_{10}$ .  $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

2. Find all solutions to the following sets of linear equations:

(a)  $7x + 3y \equiv 3 \pmod{7}$

$4x + 2y \equiv 5 \pmod{7}$

(b)  $2x + 3y \equiv 5 \pmod{8}$

$x + 6y \equiv 3 \pmod{8}$

3. Alice can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message two times, each time with a different key. Is she right? Defend your answer.

4. Alice has a long message to send. She is using the monoalphabetic substitution cipher. She thinks that if she compresses the message, it may protect the text from single-letter frequency attack by Eve. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend your answer.

5. (a) Find the result of  $00100110 \otimes 10011110$  in  $GF(2^8)$  with irreducible polynomial  $x^8 + x^4 + x^3 + x + 1$ .

- (b) Find the inverse of  $00100110$  in  $GF(2^8)$  with irreducible polynomial  $x^8 + x^4 + x^3 + x + 1$ .

6. A  $6 \times 2$  S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusive-ors the even-numbered bits to get the right bit of the output. If the input is  $110010$ , what is the output? If the input is  $101101$ , what is the output?

7. What is the key complement property in DES? How can you use this property to perform brute-force attack in  $2^{55}$  encryptions instead of  $2^{56}$  encryptions?

8. What's the purpose of Ciphertext Stealing Technique? How can it be applied to EBC mod and CBC?

9. (a) A full-size key  $n$ -bit transposition cipher can be modeled as a permutation. What's its key length? Defend your answer.

- (b) A full-size key  $n$ -bit substitution cipher can be modeled as a permutation. What's its key length? Defend your answer.

10. List the parameters (block size, key size, and the number of rounds) for the three AES versions.

Handwritten calculations for polynomial division in  $GF(2^8)$ :

Example 1:  $11110000 \div 1101$

Example 2:  $10011011 \div 1101$

Example 3:  $10011011 \div 1101$

Example 4:  $10011011 \div 1101$

Example 5:  $10011011 \div 1101$

Example 6:  $10011011 \div 1101$

Example 7:  $10011011 \div 1101$

Example 8:  $10011011 \div 1101$

Example 9:  $10011011 \div 1101$

Example 10:  $10011011 \div 1101$

Example 11:  $10011011 \div 1101$

Example 12:  $10011011 \div 1101$

Example 13:  $10011011 \div 1101$

Example 14:  $10011011 \div 1101$

Example 15:  $10011011 \div 1101$

Example 16:  $10011011 \div 1101$

Example 17:  $10011011 \div 1101$

Example 18:  $10011011 \div 1101$

Example 19:  $10011011 \div 1101$

Example 20:  $10011011 \div 1101$

Example 21:  $10011011 \div 1101$

Example 22:  $10011011 \div 1101$

Example 23:  $10011011 \div 1101$

Example 24:  $10011011 \div 1101$

Example 25:  $10011011 \div 1101$

Example 26:  $10011011 \div 1101$

Example 27:  $10011011 \div 1101$

Example 28:  $10011011 \div 1101$

Example 29:  $10011011 \div 1101$

Example 30:  $10011011 \div 1101$

Example 31:  $10011011 \div 1101$

Example 32:  $10011011 \div 1101$

Example 33:  $10011011 \div 1101$

Example 34:  $10011011 \div 1101$

Example 35:  $10011011 \div 1101$

Example 36:  $10011011 \div 1101$

Example 37:  $10011011 \div 1101$

Example 38:  $10011011 \div 1101$

Example 39:  $10011011 \div 1101$

Example 40:  $10011011 \div 1101$

Example 41:  $10011011 \div 1101$

Example 42:  $10011011 \div 1101$

Example 43:  $10011011 \div 1101$

Example 44:  $10011011 \div 1101$

Example 45:  $10011011 \div 1101$

Example 46:  $10011011 \div 1101$

Example 47:  $10011011 \div 1101$

Example 48:  $10011011 \div 1101$

Example 49:  $10011011 \div 1101$

Example 50:  $10011011 \div 1101$

Example 51:  $10011011 \div 1101$

Example 52:  $10011011 \div 1101$

Example 53:  $10011011 \div 1101$

Example 54:  $10011011 \div 1101$

Example 55:  $10011011 \div 1101$

Example 56:  $10011011 \div 1101$

Example 57:  $10011011 \div 1101$

Example 58:  $10011011 \div 1101$

Example 59:  $10011011 \div 1101$

Example 60:  $10011011 \div 1101$

Example 61:  $10011011 \div 1101$

Example 62:  $10011011 \div 1101$

Example 63:  $10011011 \div 1101$

Example 64:  $10011011 \div 1101$

Example 65:  $10011011 \div 1101$

Example 66:  $10011011 \div 1101$

Example 67:  $10011011 \div 1101$

Example 68:  $10011011 \div 1101$

Example 69:  $10011011 \div 1101$

Example 70:  $10011011 \div 1101$

Example 71:  $10011011 \div 1101$

Example 72:  $10011011 \div 1101$

Example 73:  $10011011 \div 1101$

Example 74:  $10011011 \div 1101$

Example 75:  $10011011 \div 1101$

Example 76:  $10011011 \div 1101$

Example 77:  $10011011 \div 1101$

Example 78:  $10011011 \div 1101$

Example 79:  $10011011 \div 1101$

Example 80:  $10011011 \div 1101$

Example 81:  $10011011 \div 1101$

Example 82:  $10011011 \div 1101$

Example 83:  $10011011 \div 1101$

Example 84:  $10011011 \div 1101$

Example 85:  $10011011 \div 1101$

Example 86:  $10011011 \div 1101$

Example 87:  $10011011 \div 1101$

Example 88:  $10011011 \div 1101$

Example 89:  $10011011 \div 1101$

Example 90:  $10011011 \div 1101$

Example 91:  $10011011 \div 1101$

Example 92:  $10011011 \div 1101$

Example 93:  $10011011 \div 1101$

Example 94:  $10011011 \div 1101$

Example 95:  $10011011 \div 1101$

Example 96:  $10011011 \div 1101$

Example 97:  $10011011 \div 1101$

Example 98:  $10011011 \div 1101$

Example 99:  $10011011 \div 1101$

Example 100:  $10011011 \div 1101$