Part A

1. (c) 13
2. (b) C
3. (c) EO
4. (a) CYKLU
5. (e) VXGADF
6. (b) A modified shift cipher with keyspace \{1, 2, \ldots, 25\} in which all 25 keys are equally likely.

   (d) A shift cipher in which all even keys are used with probability \(\frac{3}{25}\) and all odd keys are used with probability \(\frac{1}{25}\).
7. (c) 0011
8. (d) 0011
9. (a) 0010
10. (a) (2 marks) The study of the methods of transforming an intelligible message into one that is unintelligible and back again.

    (b) (5 marks) See page 3 of the notes.
11. (5 marks) \(9 \times 3 - 4 \times 1 = 23\) so we need the multiplicative inverse of 23.

    \[
    26 = 23 + 3 \quad 1 = 3 - 2 \\
    23 = 7(3) + 2 \quad = 3 - (23 - 7(3)) \\
    3 = 2 + 1 \quad = 8(26 - 23) - 23 \\
    \]

    So \(23^{-1} = -9 = 17 \pmod{26}\).

    \[
    K^{-1} = 17 \begin{bmatrix} 3 & -4 \\ -1 & 9 \end{bmatrix} = \begin{bmatrix} 25 & 10 \\ 9 & 23 \end{bmatrix}
    
    \]

    To decrypt \(AB\)

    \[
    \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 25 & 10 \\ 9 & 23 \end{bmatrix} = \begin{bmatrix} 9 & 23 \end{bmatrix}
    
    \]

    Thus the plaintext is jx.
12. (a) (3 marks) A polyalphabetic substitution cipher which uses a keyword of length \(m\), say \(k_1, k_2, \ldots, k_m\). To encrypt the plaintext \(x_1, x_2, \ldots\) the key is added to the plaintext, that is, \(e(x_i) = (x_i + k_i \pmod{m}) \pmod{26} = y_i\). To decrypt the ciphertext \(y_1, y_2, \ldots\) the key is subtracted from the ciphertext, that is, \(d(y_i) = (y_i - k_i \pmod{m}) \pmod{26} = x_i\).
(b) (i) (2 marks) If it were then the IC for $m = 1$ would be close to 0.065. But for $m = 1$ in the above tables we have IC = 0.048 which is closer to the value of 0.38 for random text.

(ii) (2 marks) Some of the distances between repeated substrings are 60, 24, 40, 56, 156, 184, 28, 101, 80. All of these are divisible by 4 except for 101, so we guess that the most probable keyword length is $m = 4$.

(iii) (2 marks) Since the row $m = 4$ in the second table gives IC values that are closest to 0.065, Friedman’s test tells us that $m = 4$ is the most probable keyword length.

13. (a) (2 marks) A good choice of linear recurrence relation would give a keystream with period $2^4 - 1$ for any non-zero initial key. For $l_{i+4} = l_{i+1} + l_{i+3}$ with initial key 1000 we have the keystream 10000000 . . . . Thus this is not a good choice for a linear recurrence relation.

(b) (5 marks)

| plaintext | 101010101010 |
| ciphertext | 001001011111 |
| keystream | 100011110101 |

Hence we have the equations: $l_5 = 1 = c_0$, $l_6 = 1 = c_3$, $l_7 = 1 = c_2 + c_3$, $l_8 = 1 = c_1 + c_2 + c_3$. Solving these gives $c_0 = 1$, $c_3 = 1$, $c_2 = 0$ and $c_1 = 0$. Thus the linear recurrence relation is $l_{i+4} = l_i + l_{i+3}$.

14. (a) (3 marks) $p_C(A) = p_P(c)p_K(k_2) + p_P(b)p_K(k_3)$

$$= \frac{1}{3} \times \frac{1}{3} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{1}{6}$$

(b) (3 marks) $p_P(b|A) = \frac{p_P(b)p_C(A|b)}{p_C(A)}$

$$= \frac{1/3 \times 1/6}{1/6}$$

$$= \frac{1}{3}$$

15. (a) (3 marks) A substitution-permutation cipher which takes as input a plaintext of length $2n$, where the first half is $L_0$ and the second half is $R_0$, and a key $K$ and applies $r$ rounds of processing according to the rule

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

The ciphertext is then written as $R_r L_r$.

(b) (5 marks) The 48-bit string is written as 8 6-bit strings. The $i$th 6-bit string is replaced by a 4-bit string based on the $i$th $S$-box as follows. Let the 6-bit string be $b_1 b_2 b_3 b_4 b_5 b_6$. Look up the entry in row $b_1 b_6$ and column $b_2 b_3 b_4 b_5$ of the $S$-box (where
rows are indexed by 00, 01, 10, 11 and columns are indexed by the 4-bit binary representations of the integers from 0 to 15). The entry in the $S$-box will be an integer between 0 and 15, and its 4-bit binary representation is used to replace the 6-bit string. Thus a string of length $48 = 8 \times 6$ becomes a string of length $32 = 8 \times 4$.

(c) (2 marks) The keyspace of size $2^{56}$ is not big enough to be secure. The secrecy behind the development of the $S$-boxes reduces user confidence in the system.

16. (a) (2 marks) $01001110$ and $x^6 + x^3 + x^2 + x$

(b) (4 marks) (polynomial method)

$$(x^6 + x^1)(x^4 + x^2) = x^{10} + x^8 + x^5 + x^3 + x^4 + x^2$$
$$= x^2(x^4 + x^3 + x + 1) + x^4 + x^3 + x + 1 + x^5 + x^3 + x^4 + x^2$$
$$= x^6 + x^3 + x + 1$$

(table method) \{43\} $\ast \{14\} = \{03\}^{(bd)+\{34\}} = \{03\}^{\{f1\}} = \{4b\}$

Thus the answer is $01001011$.

17. (5 marks) See proof on page 111 of the notes.