Solution of Question 1.

(a)

i It is straightforward to compute that

$$\begin{aligned} x^3 + 1 &= (x+2)\left(x^2+x+2\right) + 2x, \\ x^2 + x + 2 &= (2x+2)\,2x + 2. \end{aligned}$$

As a result,

$$1 = \gcd\left(f(x), g(x)\right).$$

[4]

ii According to the previous part, it is clear that

$$\begin{aligned} 2 &= \left(x^2+x+2\right) - (2x+2)\,2x \\ &= \left(x^2+x+2\right) - (2x+2)\left(\left(x^3+1\right) - (x+2)\left(x^2+x+2\right)\right) \\ &= (x+1)\left(x^3+1\right) + \left(1 + (2x+2)(x+2)\right)\left(x^2+x+2\right) \\ &= (x+1)\left(x^3+1\right) + \left(2x^2+2\right)\left(x^2+x+2\right) \end{aligned}$$

Multiply both sides with 2. It holds that

$$1 = (2x+2)\left(x^3+1\right) + \left(x^2+1\right)\left(x^2+x+2\right)$$

As a result,

$$\begin{aligned} a(x) &= 2x+2, \\ b(x) &= x^2+1. \end{aligned}$$

[4]

(b)

i In the given field, $x^2 + 1 = x^8$ and hence $\left(x^2+1\right)^{-1} = x^{15-8} = x^7 = x^3 + x + 1$. Therefore

$$f_1 = \left(x^2+1\right)^{-1}\left(x^3+x+1\right) = x^7 x^7 = x^{14} = x^3 + 1.$$

[4]

ii It is clear that

$$\begin{aligned} f_2 &= \left(x^3+x^2+x\right)^{-1}(x+1-x\cdot f_1) \\ &= \left(x^{11}\right)^{-1}\left(x+1+x\cdot x^{14}\right) \\ &= (x+1)(x+1+1) \\ &= x^2+x. \end{aligned}$$

[4]

(c)

i Note that $x^2+x+1=x(x+1)+1$. There is no polynomial with degree one that divides x^2+x+1 in $\mathbb{F}_2[x]$. Hence $x^2+x+1\in\mathbb{F}_2[x]$ is irreducible. [2]

ii Note that $x^2+x+1=x(x+1)+1$ and $x^2+x+1=(x+2)(x+2)$ in $\mathbb{F}_3[x]$. $x^2+x+1\in\mathbb{F}_3[x]$ is not irreducible. [2]

Solutions of Question 2.

(a) The plain text is given as

HOPE FOR THE BEST BUT PREPARE FOR THE WORST [5]

My way of cracking the cipher: I focus on three letter words. Notice that A is not far away from D or E. I tried to search the patterns matched with A*D and A*E (related to the words AND and ARE) but failed to identify them. Further notice that O is not far way from R. I searched the pattern matched with *OR and was successful. Using that information, the whole sentence can be recovered.

(b)

i Firstly, we compute the following table

x	1	2	4	8	16	32	64
17^x	17	289	173	73	42	209	141

Then we have

x	64	65	66
17^x	141	220	8

[5/7]

Hence $\log_{17} 8 = 66 \bmod 311$. [2/7]

ii Suppose that $\mathrm{ord}(a)$ does not divide 310. Then $310 = c \cdot \mathrm{ord}(a) + r$ with $0 < r < \mathrm{ord}(a)$. At the same time, $a^r = a^{310}/a^{\mathrm{ord}(a)\cdot c} = 1/1 = 1$. This contradicts the definition of $\mathrm{ord}(a)$. [3]

iii $310 = 2 \cdot 5 \cdot 31$. By the fact that $\mathrm{ord}(a) | 310$, the possible values of $\mathrm{ord}(a)$ are 1, 2, 5, 10, 31, 62, 155, and 310. [3]

iv As $\mathrm{ord}(a)$ can only be one of the eight values, we simply compute $a^x \bmod 311$ where $x \in \{1, 2, 5, 10, 31, 62, 155, 310\}$. If $a^x \neq 1 \bmod 311$ for all $x \in \{1, 2, 5, 10, 31, 62, 155, 310\} \setminus \{310\}$, then a is a primitive element. Otherwise it is not. [2]

Solutions of Question 3.

(a)

i It is straightforward to obtain

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

[2]

ii The generator matrix is given by

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

[2]

iii The syndrome vector is given by

$$\boldsymbol{s}_1 = \boldsymbol{y}_1 \boldsymbol{H}^T = [1\ 0\ 1]\,,$$

hence

$$\hat{\boldsymbol{c}}_1 = [0\ 0\ 1\ 0\ 1\ 1\ 0]\,,$$

and

$$\hat{\boldsymbol{m}}_1 = [0\ 1\ 1\ 0]\,.$$

[3]

iv The syndrome vector is given by

$$[0\ 1\ 0\ 0\ 0\ 1\ 0]\,\boldsymbol{H}^T = [1\ 0\ 1]\,.$$

Let c_3 and c_4 be the 3rd and 4th symbols in $\boldsymbol{c}$. Then one has

$$[c_3\ c_4] \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [1\ 0\ 1]\,.$$

It is clear that $[c_3\ c_4] = [0\ 1]$. Hence $\boldsymbol{c} = [0\ 1\ 0\ 1\ 0\ 1\ 0]$ and $\boldsymbol{m} = [1\ 0\ 1\ 0]$. [3]

(b)

i The distance of the code $\mathcal{C}$ is 3. [1]

ii

$$\begin{aligned} d(\mathcal{C}) &= \min_{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C},\ \mathbf{c}_1\neq\mathbf{c}_2} d(\mathbf{c}_1,\mathbf{c}_2) \\ &= \min_{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C},\ \mathbf{c}_1\neq\mathbf{c}_2} d(\mathbf{c}_1-\mathbf{c}_2) \\ &= \min_{\mathbf{c}\in\mathcal{C},\ \mathbf{c}\neq\mathbf{0}} d(\mathbf{c}), \end{aligned}$$

where the last step follows from the facts that $\mathbf{c}_1-\mathbf{c}_2\neq\mathbf{0}$, $\mathbf{c}_1-\mathbf{c}_2\in\mathcal{C}$ (by linearity), and $\{\mathbf{c}_1-\mathbf{c}_2:\ \mathbf{c}_1,\mathbf{c}_2\in\mathcal{C},\ \mathbf{c}_1\neq\mathbf{c}_2\}=\{\mathbf{c}:\ \mathbf{c}\in\mathcal{C},\ \mathbf{c}\neq\mathbf{0}\}$ (this can be verified by simply taking $\mathbf{c}_2=\mathbf{0}$). [2]

(c)

i The final results are $\mathcal{C}_a[14,4,6]$ and $\mathcal{C}_b[14,8,3]$.
It is clearly $n_a=n_b=14$.
$\mathcal{C}_a$: Every codeword $\mathbf{c}\in\mathcal{C}$ is mapped to exactly one codeword $[\mathbf{c},\mathbf{c}]\in\mathcal{C}_a$ and vice versa. Therefore, the numbers of codewords of $\mathcal{C}$ and $\mathcal{C}_a$ are exactly the same. Hence $k_a=4$. The number of nonzero elements in each codeword $\mathbf{c}_a=[\mathbf{c},\mathbf{c}]$ is exactly twice of that of the codeword $\mathbf{c}$. Therefore $d_a=6$.
$\mathcal{C}_b$: Arbitrary two codewords $\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}$ is mapped to a single codeword $\mathbf{c}_b\in\mathcal{C}_b$. The number of codewords in $\mathcal{C}_b$ is therefore $2^4\times2^4=2^8$. The dimension $k_b=8$. Note that a nonzero codeword $\mathbf{c}_b$ may be of the form of $[\mathbf{c}_1,\mathbf{0}]$ for some $\mathbf{c}_1\in\mathcal{C}$. The minimum distance of $\mathcal{C}_b$ is hence $d_b=3$.

[3]

ii It is clear that

$$\begin{aligned} \mathbf{G}_a &= [\mathbf{G},\mathbf{G}] \\ &= \begin{bmatrix} 1&0&1&1&0&0&0&1&0&1&1&0&0&0\\ 1&1&0&0&1&0&0&1&1&0&0&1&0&0\\ 1&1&1&0&0&1&0&1&1&1&0&0&1&0\\ 0&1&1&0&0&0&1&0&1&1&0&0&0&1 \end{bmatrix}, \end{aligned}$$

and

$$\mathbf{G}_b=\begin{bmatrix}\mathbf{G}&\mathbf{0}\\ \mathbf{0}&\mathbf{G}\end{bmatrix}.$$

[2]

iii Note that $\boldsymbol{G}_a$ is in the systematic form. It follows that

$$\boldsymbol{H}_a = \left[\boldsymbol{I}, \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}^T \right].$$

It can also be verified that

$$\boldsymbol{H}_b = \begin{bmatrix} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H} \end{bmatrix}.$$

[2]

Solutions of Question 4.

(a) $\forall c(x) \in \mathcal{C}$, write $c(x) = u(x)\, g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$. As cyclic codes are linear, $r(x) = c(x) - u(x)\, g(x) \in \mathcal{C}$. At the same time, $g(x) \in \mathcal{C}$ is of the least degree among all nonzero polynomials. It concludes $r(x) = 0$. Hence $c(x) = u(x)\, g(x)$. [2]

(b) Write $x^n - 1 = u(x)\, g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$. As cyclic codes are linear and $x^n - 1 \bmod x^n - 1 = 0 \in \mathcal{C}$, $r(x) \in \mathcal{C}$. By the definition of $g(x)$, the only possibility is that $r(x) = 0$. Hence $g(x) \mid (x^n - 1)$. [2]

(c)

i In this particular setting, cyclotomic cosets of 3 modulo 26 are of interest. They are

$$C_0 = \{0\}, \quad C_1 = \{1,3,9\}, \quad C_2 = \{2,6,18\}, \quad C_4 = \{4,12,10\},$$
$$C_5 = \{5,15.19\}, \quad C_7 = \{7,21,11\}, \quad C_8 = \{8.24,20\}.$$

[4]

ii

$$M^{(i)}(x) = \prod_{j \in C_i} \left(x - \alpha^j\right).$$

[1]

iii

$$\begin{aligned} g(x) &= \operatorname{lcm}\left(M^{(1)}(x), \cdots, M^{(6)}(x)\right) \\ &= M^{(1)}(x) \cdot M^{(2)}(x) \cdot M^{(4)}(x) \cdot M^{(5)}(x). \end{aligned}$$

[3]

iv $\forall c(x) \in \mathcal{C}$, it holds that $c(x) = u(x)\, g(x) = 0$ for $x = \alpha^1, \cdots, \alpha^6$. In a matrix format

$$\underbrace{\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^6 & \cdots & \alpha^{6(n-1)} \end{bmatrix}}_{\boldsymbol{A}} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \mathbf{0}.$$

Any 6-column submatrix of $\boldsymbol{A}$ is a Vandermonde matrix. This implies that any nonzero $\mathbf{c}$ contains at least $6+1$ nonzero elements. That is, $d \geq 7$. [4]

(d)

$$(x+y)^p = x^p + \sum_{i=1}^{p-1} \frac{p!}{i!\,(p-i)!} x^{p-i} y^i + y^p.$$

Note that

$$\frac{p!}{i!\,(p-i)!} = p \frac{(p-1)\cdots(p-i+1)}{i!} \in \mathbb{Z}^+.$$

At the same time, $\gcd(i!, p) = 1$. This implies that

$$\frac{(p-1)\cdots(p-i+1)}{i!} \in \mathbb{Z}^+,$$

or $p | \binom{p}{i}$. Hence $\binom{p}{i} = 0$ and $(x+y)^p = x^p + y^p$. [4]

Solutions of Question 5.

(a)

$$G_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} G_1 & 0 \\ G_1 & G_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

[2]

(b) It is clear that $I_1' = I_3' = (1-p)^2 = 0.81$ and $I_2' = I_4' = 1 - p^2 = 0.99$.

Note that U_1U_3 and Y_1Y_3 form equivalent basic building block with erasure probability $1 - 0.81 = 0.19$. Hence $I_1 = (1-0.19)^2 = 0.6561$ and $I_3 = 1 - 0.19^2 = 0.9639$. Similarly, U_2U_4 and Y_2Y_4 form equivalent basic building block with erasure probability $1 - 0.99 = 0.01$. Therefore $I_2 = (1-0.01)^2 = 0.9801$ and $I_4 = 1 - 0.01^2 = 0.9999$. [4]

(c) $[?, y_2]$ is decoded to $[u_1, u_2] = [?, y_2]$.

$[y_1, ?]$ is decoded to $[u_1, u_2] = [?, ?]$ as there is no sufficient information to decode either u_1 or u_2.

In this example, it is clear that U_2 is more reliable than U_1. [4]

(d) $[?, y_2, y_3, y_4]$ is decoded to $[?, y_2 + y_4, y_3 + y_4, y_4]$.

$[y_1, ?, y_3, y_4]$ is decoded to $[?, ?, y_3 + y_4, y_4]$.

$[y_1, y_2, ?, y_4]$ is decoded to $[?, y_2 + y_4, ?, y_4]$.

$[y_1, y_2, y_3, ?]$ is decoded to $[?, ?, ?, ?]$.

The most reliable symbol is U_4 and the lest reliable one is U_1. [5]

(e) $[?, y_2, y_3, y_4]$ is decoded to $[0, y_2 + y_4, y_3 + y_4, y_4]$.

$[y_1, ?, y_3, y_4]$ is decoded to $[0, y_1 + y_3, y_3 + y_4, y_4]$: Note that $u_1 + u_2 + u_3 + u_4 = y_1$. Substitute $u_1 = 0$, $u_3 = y_3 + y_4$, and $u_4 = y_4$. One has $u_2 = y_1 + y_3$.

$[y_1, y_2, ?, y_4]$ is decoded to $[0, y_2 + y_4, y_1 + y_2, y_4]$: Substitute $u_1 = 0$, $u_2 = y_2 + y_4$, and $u_4 = y_4$ into $u_1 + u_2 + u_3 + u_4 = y_1$. One has $u_3 = y_1 + y_2$.

$[y_1, y_2, y_3, ?]$ is decoded to $[0, y_1 + y_3, y_2 + y_3, y_1 + y_2 + y_3]$: This result can be obtained by using the following equations $u_2 + u_3 + u_4 = y_1$, $u_2 + u_4 = y_2$, and $u_3 + u_4 = y_3$. [5]