CS698G Assignment 1

Roll Number: 230643

Question 1

(a)

1. $\Pr(P = p)$
2. $\Pr(C = c \mid P = p) \cdot \Pr(P = p) / \Pr(C = c)$
3. —
4. $\frac{1}{2^n}$
5. $\frac{1}{2^n} \cdot \frac{1}{2^n}$
6. $\frac{1}{2^n}$

(b)

$$\boxed{\mathrm{C}_2 = P_2 \oplus K}$$

$$\boxed{\mathrm{C}_1 \oplus C_2 = P_1 \oplus P_2}$$

We can simply XOR this with a guessed value to check if it yields a valid string like `"email"`. If not, then the plaintext is the other option (`"hello world"`). Converting everything to hex

$$c1 = 0001100000010111000001010000000100001010 = 0x18, 0x17, 0x05, 0x01, 0x0A$$

$$c2 = 0000011100011101000110110000000100000001 = 0x07, 0x1D, 0x1B, 0x01, 0x01$$

$$c1 \oplus c2 = 0x1F, 0x0A, 0x1E, 0x00, 0x0B$$

$$hello = \{0x68, 0x65, 0x6C, 0x6C, 0x6F\}$$

$$world = \{0x13, 0x0C, 0x0D, 0x1C, 0x09\}$$

$$hello \oplus world = 0x1F, 0x0A, 0x1E, 0x00, 0x0B$$

This matches $c1 \oplus c2$ thus,

$$\boxed{\text{c1 = “hello” and c2 = “world”.}}$$

Cross-checking for ”value” and ”email”:

$$value = 0x76, 0x61, 0x6C, 0x75, 0x65$$
$$email = 0x65, 0x6D, 0x61, 0x69, 0x6C$$
$$value \oplus email = 0x13, 0x0C, 0x0D, 0x1C, 0x09$$

which obviously does not match with $c1 \oplus c2$.

(c)

Since $p, k \in \mathbb{Z}_n$ and n is prime, k^{-1} exists.

Decryption formula:

$$\boxed{\text{C } \cdot K^{-1} \bmod n}$$

It is not secure because the multiplicative inverse K^{-1} is guaranteed to exist and can be computed efficiently.

(d)

On converting the given ciphertext from hexadecimal to bytes:

```
\x1c\x05G\x1c\x0e\x00U\x1b\t\x15\x1dO\x17\x1cU\x0bO\x16O
\x13\x01\x01\x1c\x1d\x00\x0e\x04
n do for you, ask what you can do for your country. JFK
```

As given in the question, the key is not a block cipher; thus, the rest of the text is the plaintext. The obvious guess for the complete plaintext is the famous quote by JFK, *“Ask not what your country can do for you, ask what you can do for your country.”*

We can obtain the key by applying XOR on the encrypted part of the text with “ask not what your country ca”

Key: `congratulations you found me`

Plain Text: Ask not what your country can do for you, ask what you can do for your country.

Question 2

(a)

Decryption function:

$$\boxed{\text{p} \equiv a^{-1} \cdot c - b \pmod{28}}$$

Working (assuming a^{-1} exists):

$$c \equiv a(p + b) \;\Rightarrow\; a^{-1}c = p + b \;\Rightarrow\; p \equiv a^{-1}c - b \pmod{28}$$

(b)

For a^{-1} to exist, a must be coprime to 28.

$$\boxed{\phi(28) = \phi(2^2 \cdot 7) = \phi(4)\,\phi(7) = (4-2)(7-1) = 2 \cdot 6 = 12.}$$

So, 12 choices for a, and 28 choices for b.
Total keys: $28 \times 12 = 336$.

$$\boxed{\text{Non-trivial keys: } 336 - 1 = 335}$$

(excluding $a = 1, b = 0$).

(c)

Let $H(p)$ be the helper function returning ciphertext c. We know:

$$c \equiv a(p+b) \pmod{28},$$

$$H(0) = ab \bmod 28$$

$$H(1) = a(1+b) = a + ab \bmod 28.$$

Hence

$$\boxed{\text{H(1) - H(0) = a mod28}}$$

$$\boxed{\text{b = a}^{-1}H(0)\text{ mod 28.}}$$

(again assuming a^{-1} exists). You compute a^{-1} via the extended Euclidean algorithm.

Question 3

Initially, I calculated the frequency of all characters. Most frequent: `‘m’` must be the space character. Next: `‘l’` should be ‘e.’according to the frequency analysis chart of the english alphabets.

Modified text: - ‘space’ → `$` - Changed guessed characters to capital letters

First filtered line: `"vsl qlfx 1866"`
Guess: `"THE YEAR 1866"`

From ”kY” and ”Ay T$”, I guessed $\boxed{k = B,\, y = S,}$ $ = O. (Resemblance to ”by” and ”as to” which are common phrases)

”rHIzH” implies $\boxed{r = W,\, z = C.}$ (Resemblance to ”which”)

Then observed encrypted words like:

- ”CnASSIc, IT Ic THE nIST Oi” $\boxed{n = L,\, c = N,\, i = F, \text{ and } , = G}$
- ”SpeERcATpRAL AeeARITIOca” $\boxed{p = U,\, e = P,\, a = .}$ (full stop)

(Resemblance to ”classing it in the list of” and ”supernatural apparition”)
Following up on such words, I ended up with this as first line: Final partial line:

> THE YEAR 1866 WAS SIGNALIZED BY A REMARKABLE INCIDENT,
> A MYSTERIOUS AND PUwwLING PHENOMENON,

From words like ”EtCITEMENT”, ”FAdOUR”, ”.UESTION”, ”PUwwLING”:

$$\boxed{\text{d} = \text{V}, \quad \text{t} = \text{X}, \quad . = \text{Q}, \quad \text{w} = \text{Z}}$$

On further filtering, and finding resemblance to common english words, the text was completely decrypted.

Final Decrypted Text

```
THE YEAR 1866 WAS SIGNALISED BY A REMARKABLE INCIDENT, A MYSTERIOUS AND PUZZLING
PHENOMENON, WHICH DOUBTLESS NO ONE HAS YET FORGOTTEN. NOT TO MENTION RUMOURS
WHICH AGITATED THE MARITIME POPULATION AND EXCITED THE PUBLIC MIND, EVEN IN
THE INTERIOR OF CONTINENTS, SEAFARING MEN WERE PARTICULARLY EXCITED. MERCHANTS,
COMMON SAILORS, CAPTAINS OF VESSELS, SKIPPERS, BOTH OF EUROPE AND AMERICA,
NAVAL OFFICERS OF ALL COUNTRIES, AND THE GOVERNMENTS OF SEVERAL STATES ON THE
TWO CONTINENTS, WERE DEEPLY INTERESTED IN THE MATTER. FOR SOME TIME PAST, VESSELS
HAD BEEN MET BY "AN ENORMOUS THING," A LONG OBJECT, SPINDLE-SHAPED, OCCASIONALLY
PHOSPHORESCENT, AND INFINITELY LARGER AND MORE RAPID IN ITS MOVEMENTS THAN
A WHALE. THE FACTS RELATING TO THIS APPARITION (ENTERED IN VARIOUS LOG-BOOKS)
AGREED IN MOST RESPECTS AS TO THE SHAPE OF THE OBJECT OR CREATURE IN QUESTION,
THE UNTIRING RAPIDITY OF ITS MOVEMENTS, ITS SURPRISING POWER OF LOCOMOTION,
AND THE PECULIAR LIFE WITH WHICH IT SEEMED ENDOWED. IF IT WAS A CETACEAN, IT
SURPASSED IN SIZE ALL THOSE HITHERTO CLASSIFIED IN SCIENCE. TAKING INTO CONSIDERATION
THE MEAN OF OBSERVATIONS MADE AT DIVERS TIMES,€"REJECTING THE TIMID ESTIMATE
OF THOSE WHO ASSIGNED TO THIS OBJECT A LENGTH OF TWO HUNDRED FEET, EQUALLY
WITH THE EXAGGERATED OPINIONS WHICH SET IT DOWN AS A MILE IN WIDTH AND THREE
IN LENGTH,€"WE MIGHT FAIRLY CONCLUDE THAT THIS MYSTERIOUS BEING SURPASSED GREATLY
ALL DIMENSIONS ADMITTED BY THE ICHTHYOLOGISTS OF THE DAY, IF IT EXISTED AT
ALL. AND THAT IT DID EXIST WAS AN UNDENIABLE FACT; AND, WITH THAT TENDENCY
WHICH DISPOSES THE HUMAN MIND IN FAVOUR OF THE MARVELLOUS, WE CAN UNDERSTAND
THE EXCITEMENT PRODUCED IN THE ENTIRE WORLD BY THIS SUPERNATURAL APPARITION.
AS TO CLASSING IT IN THE LIST OF FABLES, THE IDEA WAS OUT OF THE QUESTION.
```

Character Map (C++ Code)

```
mp['m'] = '-';
mp['l'] = 'E';
mp['v'] = 'T';
mp['r'] = 'W';
mp['k'] = 'B';
mp['f'] = 'A';
mp['y'] = 'S';
mp['-'] = 'O';
mp['x'] = 'R';
mp['s'] = 'H';
mp['q'] = 'Y';
```

```
mp['o'] = 'I';
mp['b'] = 'J';
mp['z'] = 'C';
mp['n'] = 'L';
mp['i'] = 'F';
mp['c'] = 'N';
mp[','] = 'G';
mp['h'] = 'D';
mp['e'] = 'P';
mp['p'] = 'U';
mp['j'] = 'M';
mp['g'] = 'K';
mp['u'] = ',';
mp['a'] = '.';
mp['t'] = 'X';
mp['d'] = 'V';
mp['.'] = 'Q';
mp['w'] = 'Z';
```

Rest characters are left the same.

Question 4

(b)

We assume at most n consoles, viewed as leaves of a full binary tree of height $\log_2 n$. Each node v has a permanent secret key k_v. Console i stores the keys along the unique path

$$S_i = \{\, v_{i,0}, v_{i,1}, \ldots, v_{i,\log_2 n}\}$$

from the root $v_{i,0}$ to leaf i. A game message m is encrypted under a fresh content key $k \in \mathcal{K}$ as

$$\text{Header} \,\|\, \text{Body} \;=\; E(k_{\mathsf{root}},\, k) \,\|\, E(k,\, m).$$

Since every console knows k_{root}, all can decrypt k and then m.

Suppose a set of hacked consoles

$$I = \{\, i_0, i_1, \ldots, i_{s-1}\}, \quad s > 1,$$

have their embedded keys fully exposed. We must *revoke* exactly those consoles from decrypting *new* game releases while allowing all others to decrypt.

We construct a *cover set* $\mathcal{C}$ of tree-nodes whose subtrees exactly cover the non-revoked leaves. The size of $\mathcal{C}$ will be $O(s \log n)$.

1. Initialize $\mathcal{C} \leftarrow \{\rho\}$, where ρ is the root.
2. For each revoked console $i_j \in I$:
   (a) Let $\text{Path}(i_j) = (\rho = v_{j,0}, v_{j,1}, \ldots, v_{j,\log n})$.
   (b) Traverse v along this path from root downward:

```
if $v \in \mathcal{C}$ then
    Remove $v$ from $\mathcal{C}$.
    Let $v_{\text{sb}}$ be the sibling of $v$.
    Add $v_{\text{sb}}$ to $\mathcal{C}$.
    Break (stop processing this path).
end if
```

To encrypt a new game m:

1. Sample fresh content key $k \leftarrow \mathcal{K}$.
2. For each $v \in \mathcal{C}$, compute ciphertext
$$C_v \;=\; E(k_v,\, k).$$
3. Form the header:
$$\text{Header} \;=\; \big\{(v,\, C_v) \colon v \in \mathcal{C}\big\}.$$
4. The body remains $E(k, m)$.

Decryption: A non-revoked console $i \notin I$ knows the keys on its path S_i. There is exactly one node $v \in \mathcal{C} \cap S_i$. The console finds (v, C_v), computes $k = D(k_v, C_v)$, then $m = D(k,\, E(k, m))$.

Complexity:

- $\lvert\mathcal{C}\rvert = O(s \log n)$, so the header contains $O(s \log n)$ short ciphertexts.
- Each non-revoked console performs one symmetric-key decryption to recover k, then one more to recover m.
- Revocation processing and header assembly cost $O(s \log n)$ time.

Conclusion: This scheme achieves selective revocation with header size $O(s \log n)$, allowing precisely the non-revoked consoles to decrypt new game content.

(a)

For part (a), everything in part (b) can be repeated for I.size() = 1
We go down the path from root to i say,

$$\boxed{\text{Path(i)} = (\rho = v_{j,0}, v_{j,1}, \ldots, v_{j,\log n})}$$

Replace each node in path to its sibling (since it is a complete binary tree siblings always exist except for leaf)

- **Revoked console** i lacks all sibling-keys k_v for $v \in \mathcal{C}$ and thus cannot recover k.
- $\lvert\mathcal{C}\rvert = \log_2 n$, so the header contains $\log_2 n$ short ciphertexts.
- Each non-revoked console performs exactly one decryption of C_v and then one decryption of the body.

Hence the game m is securely encrypted with a header of size $O(\log n)$, disabling only console i.