CS698G Assigment 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)

$$C_1 = P_1 \oplus K, \quad C_2 = P_2 \oplus K$$

$$C_1 \oplus C_2 = P_1 \oplus P_2$$

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 (e.g., `"hello world"`).

(c)

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

Decryption formula:

$$C \cdot K^{-1} \mod n$$

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

(d)

The key size is much smaller than the ciphertext. Since the key repeats every 28 characters and is a famous English phrase, it is prone to attacks of cryptanalysts.

By 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\x04n do for you,
ask what you can do for your country. JFK
```

It is hinted that the plaintext is a JFK quote. Using `"ask not what your country ca"` as the cyclic key, we obtain the original key and plaintext:

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:

$$p = a^{-1} \cdot c - b \mod 28$$

Working:

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

(b)

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

$$\phi(28) = \phi(2^2 \cdot 7) = \phi(4) \cdot \phi(7) = (4-2)(7-1) = 2 \cdot 6 = 12$$

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

Non-trivial keys: $336 - 1 = 335$ (excluding $a = 1, b = 0$)

(c)

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

We know:

$$c = a(p + b) \mod 28$$

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

$$H(1) = a(1 + b) = a + ab \Rightarrow H(1) - H(0) = a$$

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

Compute a^{-1} using extended Euclidean algorithm.

Question 3

Initially, I calculated the frequency of all characters. Most frequent: `'m'` space character. Next: `'l'` 'e'.

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

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

From "kY", "Ay T$" $k = B$, $y = S$, \$ = O.

"rHIzH" implies $r = W$, $z = C$.

Then observed:

- "CnASSIc, IT Ic THE nIST Oi" $n = L$, $c = N$, $i = F$, ',' = G
- "SpeERcATpRAL AeeARITIOca" $p = U$, $e = P$, $a =$. (full stop)

Final partial line:

> THE YEAR 1866 HAS SIGNALISED BY A REMARKABLE INCIDENT, A MYSTERIOUS AND PUZZLING PHENOMENON,

From words like "EtCITEMENT", "FAdOUR", ".UESTION":

$$d = V, \quad t = X, \quad . = Q$$

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,óé¼Ç¥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,óé¼Ç¥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';
```

Question 4

(a)

If the i-th console is hacked:

- Secure the i-th console.
- Secure others by removing all keys on the path from root to i.

In a complete binary tree, every node on path root $\rightarrow i$ has a sibling which is root of a subtree excluding i.

Encrypt content key using one key from each such sibling node. Console i holds no valid headers.

(b)

Let I be the set of compromised consoles. Mark each as revoked.

Traverse each node:

- If the subtree contains any revoked node, mark separately.
- If all leaves in subtree are revoked, skip.
- Else, for each selected node, put $E(key_{node}, k)$ in header.

Each revoked leaf causes a split at every level $O(s)$ selected nodes per level, thus $O(s \log n)$ ciphertexts in total.