Alay Shah — Homework 1 — CS 579
10433839 — Foundations of Cryptography

Problem 1

1. Substitution Cipher – Substitution cipher is a method in which each unit from the plaintext is substituted with the unit of ciphertext. The units may be single letters, pairs, triples or so on depending upon the agreeing terms.

Message Space → {∀c ∈ A}
Gen → It is an algorithm which generates the key to encrypt and decrypt the text.

Enc → It is an algorithm which means that if one message is encrypted multiple times, it may yields a different ciphertext every time.

Dec → It is an algorithm which means that whichever is the ciphertext, it will yield the correct message from it.

2. Frequency analysis from Figure 1:
CRYPTOGRAPHICSYSTEMESAREEXTREMELYDIFFICULTTOBUILDNEVERTHELESSFOR
SOMEREASONMANYNONEXPERTSINSISTONDESIGNGNEWENCRYPTIONSCHEMESTHA
TSEEMTMTHEMTOBEMOREMORESECURETHANANYORHERSCHEMEONEARTHTHEUN
FORUNATETRUTHHOWEVERISTHATSUCHSCHEMESAREUSUALLYTRIVIALTOBREAK

Letters	Frequency	Percentage
A	3	1.22
B	12	4.91
C	3	1.22
D	2	0.81
E	4	1.63
F	37	15.16
G	19	7.78
H	14	5.73
I	9	3.68
J	9	3.68
K	3	1.22
L	17	6.96
M	4	1.63
N	0	0
O	16	6.55
P	10	4.09
Q	26	10.65
R	7	2.86
S	2	0.81
T	0	0
U	0	0
V	15	6.14
W	21	8.61
X	1	0.41
Y	3	1.22
Z	7	2.86

Comparing the above the frequency analysis and the frequency histogram provided in figure 2, we can assume that E is mapped to F (highest frequency in both), T is mapped to Q (second highest frequency) and so on.

Mapped elements are:

A	3	1.22	X	2
B	12	4.91	D	4.3
C	3	1.22	O	1.9
D	2	0.81	U	1
E	4	1.63	F	2.2
F	37	15.16	E	12.7
G	19	7.78	I	7
H	14	5.73	Q	6
I	9	3.68	C	2.8
J	9	3.68	T	2.8
K	3	1.22	B	1.5
L	17	6.96	Z	6.7
M	4	1.63	G	2
N	0	0	W	0.2
O	16	6.55	R	6.3
P	10	4.09	L	4
Q	26	10.65	S	9.1
R	7	2.86	M	2.4
S	2	0.81	K	0.8
T	0	0	P	0.1
U	0	0	Y	0.1
V	15	6.14	H	6.1
W	21	8.61	A	8.2
X	1	0.41	J	0.2
Y	3	1.22	N	1.5
Z	7	2.86	V	2.4

Plaintext: CRYPTOGRAPHIC SYSTEMES ARE EXTREMELY
DIFFICULTTOBUILDNEVERTHELESSFORSOMEREASONMANYNONEXPERTSINSISTONDESIG
NGNEWENCRYPTIONSCHEMESTHATSEEMTMTHEMTOBEMOREMORESECURETHANANYOR
HERSCHEMEONEARTHTHEUNFORUNATETRUTHHOWEVERISTHATSUCHSCHEMESAREUSUA
LLYTRIVIALTOBREAK

3. For substitution cipher, it is possible to use a chosen-plaintext attack with a carefully selected plaintext which contains at least 25 distinct letters, provided the ciphertext for the same, it is then possible to find the key and encrypt and decrypt all the other plaintexts and ciphertexts.

4. IF K (key) is randomly chosen from the key space of size 26! An attacker may choose any K, but it is impossible to gain a certain profit by that. Each M (message) and C (ciphertext) is equally likely as before.

Problem 2:

1. Consider Π = (Gen, Enc, Dec) be a one-time pad cipher. Π' = (Gen, Enc', Dec')
   Now, Dec' simply truncates the last bit from the ciphertext and will use Dec to decrypt the ciphertext. Therefore, Π' is correct if Π is. Also, if ciphertext distribution of Π does not depend on message then Π' does not too, as it is the same distribution with a bit appended and the bit is independent of the message and hence, Π' is perfectly secret. However, ciphertext distribution of Π' is not uniform as ciphertexts ending with 0 (0.65) are two times as likely as ciphertexts ending with 1 (0.3). And thus, it contradicts the condition.

2. Encryption is perfectly secret if ciphertext distribution doesn't depend on the message. The condition stated Pr[C = c0] = Pr[C = c1] implies that every message induces the uniform ciphertext distribution.

Problem 3:

1. v1(n) is negligible
   p(.) is a positive polynomial

   Now,
   As v1 is negligible, it is smaller than the inverse of any other polynomial, for all large n. Therefore, for any given polynomial q,
   v1 <= 1/pq
   And hence, v2(n) < 1/pq
   Therefore, v2(n) = p(n) . n1(n) is also negligible

2. v(n) = $\frac{n^{10^5}}{2^{n^{1/2}}}$
   Here, n is any positive integer. Considering numerator, 10^5 is 100000. Power of n to 100000 is a very significant number. Irrespective of the denominator, the value of v(n) is not negligible. And hence, v(n) is not a negligible function.

   v(n) = $\frac{n^{-5^{10}}}{10^5 \,.\, n^{10^5}}$
   Here, n is any positive integer. Considering numerator, -5^{10}. Power of n being negative, it leads to being in the denominator. Leaving numerator as 1. Denominator becomes $n^{-5^{10}} \,.10^5 \,.\, n^{10^5}$ which is a very significant number and hence, v(n) is a negligible function.

Problem 4:

1. If |m0| = |m1| we get a cipher text c_b.
For the attack, the probability is at most 0.5 + ε(n) where ε is a negligible function.
Hence, no possible attacker can compute b correctly non-negligibly better than a random guess.

2. Π' is defined over Message Space M = {0,1}*
p(.) is upper bound to time spent on Enc' → negligible function
Now, if m0 ∈ {0,1}
m1 ∈ $\{0,1\}^{p(n) + c}$
As p(n) is negligible → $\{0,1\}^{c}$
c is a positive integer >= 1.

So, the probability of m0 will be 0.5 + ε0(n) where ε0 is a negligible function and for m1 will be 0.5 + ε1(n) where ε1 is also a negligible function.
When the probability for m0 and m1 is 0.5 each, it will result in an easy attack by the attacker.

3. Π' = (Gen', Enc', Dec') Message Space → M'
Π = (Gen, Enc, Dec) Message Space → M
Assume Enc' → m' ∈ M' merely applies Enc
Enc → m = E(m') ∈ M of m'