Homework 1

1 Problem 1 (20 points)

Each of the following ciphertexts were encrypted using one of the following types of ciphers:

1. A shift cipher
2. A simple (monographic, monoalphabetic, non-homophonic) substitution cipher (but not a shift cipher)
3. A Vigenère cipher
4. A Transposition Cipher

For each ciphertext below, guess which of the ciphers were used to encrypt. You do not need to determine the plaintext or the key. Explain your reasoning. The plaintext is standard English text with all spaces and punctuation removed and upper/lower case ignored. Each cipher is used to generate exactly one ciphertext. For your convenience, the letter counts in each ciphertext are given.

(a)
```
"RVSQUYQZGSUTIUWFSYMDZGVFZQRZUYOWXFSIZYSGQWXCRUMWOCVXOGRVSOWRUI
LWZRZYMUWGUDPZYMQUFSGRVZGZGVZGRUWZQODDXOQQKWORSHKRFUSGYURQOCRKWS
RVSQKWWSYRHWSOFRVUIRVSIZSDFUWZRGCWSGSYRFOXGQZSYRZIZQIUKYFORZUYGR
VSFSIZYZRZUYIUQKGSGGUDSDXUYRVSQUFSGRVORVOPSHSSYKGSFIUWQSYRKWZSGR
USYOHDSGSQWSRQUBBKYZQORZUY"
```

A	B	C	D	E	F	G	H	I	J	K	L	M
0	2	4	8	0	12	21	4	10	0	9	1	4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	15	2	18	29	34	1	25	13	18	6	20	24

(b)
```
"BPPANSCTIAHNORTYIOASKOSTCULNTNTICDIATPELAROUTDYAVTDTICEEGARNMI
UMIADRRROSPMRTDIHSSIIHSCNEPOATNSRUSESAAEUMTIMCTTWAMCGIETMATQRIIF
ITDICAATSACGNYMSONTWCMNGRCEXIRSCRNIRTANLNTHROEGVOECAESTNOYVSFMLI
ORGNTSNRDTSSRLUTHDCSHHSLMIRIETQRNEETFHASEIIDIGAMTTIRAERINLHEPPOH
YHCHSCDLMSSSTPOIVITOYAOEMAISESENGEUEGCYOOETECCOEOISOHTNOCTAZWDAR
```

THLEOEANFUIIAYATEUNNEAYAWEAUEHETAFUNTNFHGTRLUIGEOCACDLNWTPODPHEI
OYORRNSUATEUSNTOOEDBOTGAAT"

A	B	C	D	E	F	G	H	I	J	K	L	M
36	2	22	14	36	6	12	17	34	0	1	11	14
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
28	29	10	2	25	30	44	14	4	5	1	10	1

(c) "VPTKMTVQDUEIALTMMEKBXVRRNADYIWGZHASTTGEASXTIEOCRUICHVKWVIPPCCB
TPRKJMIDIEVQTALTGVIBVPEZNWXFIZPWLPYIHPRUGMSSEIIMAFEECZIJSEUBGBGK
KVVNSFFKDKIJQZQYIRMQCNIOKAIPRXQVTZVVNQTKSEEZTHXZXQIFEEFISLZVNWEL
HJGVHLSWJWLJSUGALVVBVPTYINCAAPXKNMIOIFTGIVVVNGDUEEFNDYECQVVAMDGV
DDSIMQCNHVHQCPXZQVDMAYCBRVRJVQIBXVUIVVSU"

A	B	C	D	E	F	G	H	I	J	K	L	M
12	8	11	10	18	8	11	8	26	7	1	8	11
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	3	12	13	9	12	14	8	31	7	9	6	10

(d) "XACEJJEJCEJPDAJEJAPAAJOARAJPEAOWJZJEJAPAAJAECDPEAOPDEOLEYPQNAK
BYNULPKCNWLDUNWZEYWHHUYDWJCAZWNEYDPDAKNUXACWJPKAIANCAAJWXHEJCPDA
NECKNKQOOPQZUKBYNULPKCNWLDUWOWOYEAJYAWJZWIWPDAIWPEYWHZEOYELHEJAP
DEOLANOLAYPERADWOEJPQNJEJBHQAJYAZDKSNAOAWNYDANOPDEJGWXKQPPDAXNKW
ZANBEAHZKBYKILQPANOAYQNEPU"

A	B	C	D	E	F	G	H	I	J	K	L	M
39	5	10	16	26	0	1	7	4	24	13	9	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	15	23	8	2	1	0	8	0	20	5	15	9

Bonus (10 points): For the ciphertext encrypted using a Vigenère cipher, determine the key length

2 Problem 2 (50 points)

Each of the following describes the encryption algorithm for a potential encryption scheme. For each scheme, decide if the scheme represents a perfectly secure encryption scheme. If yes, prove that the scheme is perfectly secure. If not, explain what fails. Be as precise as possible. If the scheme is not perfectly secure, describe the attack. If the scheme is not a valid encryption scheme, explain why. There may be more than one thing wrong with the scheme — if so, you should explain all the ways in which it is incorrect. Efficiency is not a consideration.

(a) Messages are ℓ bits, and keys are random ℓ bit strings.

$$\mathsf{Enc}(k, m) = (k \oplus m)||(k \oplus c)$$

Here, c is a fixed ℓ-bit constant that is part of the description of Enc.

(b) Messages are ℓ bits, and keys are random ℓ bit strings.

$$\mathsf{Enc}(k, m) = (k \oplus m)||(k \oplus r)$$

Here, r is a random ℓ-bit string that is chosen when encrypting m: the string r is not a part of the description of Enc, and is chosen freshly at random every time a message is to be encrypted.

(c) Messages are ℓ bits, and keys are random ℓ bit strings.

$$\mathsf{Enc}(k, m) = (k \oplus r)||(r \oplus m)$$

Here, r is a random ℓ-bit string that is chosen when encrypting m: the string r is not a part of the description of Enc, and is chosen freshly at random every time a message is to be encrypted.

(d) Messages are ℓ bits, and keys are random 2ℓ-bit strings.

$$\mathsf{Enc}(k, m) = k \oplus (m||c)$$

That is, to encrypt, append c to m, and then XOR the resulting 2ℓ-bit string with k. Here, c is a fixed ℓ-bit constant that is part of the description of Enc.

(e) Messages are ℓ bits, and keys are random 2ℓ-bit strings.

$$\mathsf{Enc}(k, m) = k \oplus (m||r)$$

That is, to encrypt, append r to m, and then XOR the resulting 2ℓ-bit string with k. Here, r is a random ℓ-bit string that is chosen when encrypting m: the string r is not a part of the description of Enc, and is chosen freshly at random every time a message is to be encrypted.

(f) Messages are ℓ bits, and keys are random ℓ-bit strings.

$$\mathsf{Enc}(k, m) = (k \oplus m)||(k \oplus m)$$

That is, XOR k and m, and write down the resulting string twice.

(g) Messages are ℓ bits, and keys are random permutations on ℓ items. $\mathsf{Enc}(k, m)$ shuffles the bits of m using the permutation described by k.

(h) Messages are ℓ bits, and keys are random ℓ bit strings. $\mathsf{Enc}(k, m)$ is the bit-wise AND of k and m.

(i) Messages are ℓ bits, and keys are random ℓ-bit strings. To encrypt, scan through the bits of k and m. If the ith bit of k is 0, delete the ith bit of m. If the ith bit of k is 1, keep the ith bit of m. The ciphertext is the remaining bits of m that were not deleted. As an example, to encrypt `"11010100"` using the key `"10110010"`, we would keep the first, third, fourth and seventh bit of the message, so the ciphertext would be `"1010"`.

(j) Messages are ℓ bits, and keys are random ℓ-bit strings. To encrypt, scan through the bits of k and m. If the ith bit of m is 0, delete the ith bit of k. If the ith bit of m is 1, keep the ith bit of k. The ciphertext is the remaining bits of k that were not deleted. As an example, to encrypt `"11010100"` using the key `"10110010"`, we would keep the first, second, fourth and sixth bit of the key, so the ciphertext would be `"1010"`.

(k) Messages are ℓ bits, and keys are random 2ℓ-bit strings. Interpret the key k as two ℓ bit strings: k_0 and k_1. Scan through the bits of k_0, k_1 and m. If the ith bit of m is 0, write down the ith bit of k_0 and discard the ith bit of k_1. If the ith bit of m is 1, write down the ith bit of k_1 and discard the ith bit of k_0. In other words, the ith bit written down is $(k_{m_i})_i$. The ciphertext is the resulting ℓ bit string. As an example, to encrypt `"11010100"` using the key $k_0 =$`"10110010"` and $k_1 =$`"11001010"`, we will write down the first, second, fouth, and sixth bits of k_1 and the third, fifth, seventh, and eighth bits of k_0, giving the ciphertext `"11100010"`.

3 Problem 3 (15 points)

(a) Devise an encryption scheme such that (1) given an encryption of any message, an adversary can figure out 90% of the secret key, but (2) the scheme is still perfectly secure, despite 90% of the key being revealed. Do not forget to prove that the scheme is secure and that it is correct.

(b) Devise an encryption scheme such that (1) given an encryption of any message, an adversary learns *nothing* about the secret key, but (2) the scheme is completely broken (as in, given the ciphertext, an adversary can completely recover the plaintext).

4 Problem 4 (15 points)

Consider the following security notion for an encryption scheme:

Definition 1. *An encryption scheme* ($\mathsf{Enc}, \mathsf{Dec}$) *for ℓ-bit messages is* half-message perfectly secure *if, for any two ℓ-bit messages m_0, m_1 such that m_0* and *m_1* agree on at least $\ell/2$ bits*, the distributions* $\mathsf{Enc}(k, m_0)$ *and* $\mathsf{Enc}(k, m_1)$ *are identical.*

This is the same definition as perfect security seen in class, except for the restriction that it only applies to m_0, m_1 that agree on at least $\ell/2$ bits. Therefore, it is a seemingly weaker definition.

Prove that any encryption scheme that is *half-message perfectly* secure must in fact also be *perfectly* secure.

[Hint: for any two messages m_0, m_1, come up with a new message m_2. Then apply half-message perfect security twice, once for m_0, m_2, and then again for m_2, m_1.]