Assignment 1: Cryptography

1 Alphabetic Substitution

The following text has been encoded by an *alphabetic substitution* cipher. That means, that the ciphertext alphabet contains the same letters as the plaintext alphabet, but the order of the letters has been scrambled. This is a *mono alphabetic* substitution cipher.

```
LYMBXJXKBBKBJPJJBBKBJPZPHYXNJKGOLOGPIEYHKBI
XJSOEPVJBPMBXJEPONKBIEJGJOEATPYOXUOBAJPTJLK
JDXGYLOEPKLKAKODKBPJDDKIJBAJXOPOGAKJBAJAYVS
MPJEGAKJBAJOSSDKJXVOPTJVOPKAGOBXEYFYPKAGLME
PTJEVYEJXNJVOKBPOKBGODOEIJBJPHYENYLKBXMGPEZ
SOEPBJEGPTEYMITPTJOHOEXHKBBKBINJHYENSEYIEOV
VJOBXPTEYMITYMEEJGJOEATAYDDOFYEOPKYBGPTJXJS
OEPVJBPSEYUKXJGJXMAOPKYBPTEYMITYBJFOATJDYEG
SEYIEOVVJOBXPHYVOGPJEGSEYIEOVVJGEJGJOEATOPP
TJXJSOEPVJBPYLXOPOGAKJBAJOBXNBYHDJXIJJBIKBJ
JEKBIGSOBGPTJXKGAKSDKBJGOBXKBPJELOAJGYLOEPK
LKAKODKBPJDDKIJBAJXOPOGAKJBAJAYVSMPJEGAKJBA
JOBXOSSDKJXVOPTJVOPKAGHJXJUJDYSBJHPYYDGOBXV
JPTYXYDYIKJGPYOXUOBAJPTJGJLKJDXGOPPTJGOVJPK
VJHJAYDDOFYEOPJHKPTOHKXJEOBIJYLKBGPKPMPJGFY
PTHKPTKBOBXYMPGKXJYLVOOGPEKATPMBKUJEGKPZOBX
HYENYBXKUJEGJOSSDKAOPKYBGKBADMXKBIKBPTJLKJD
XGYLTJODPTOBXVJXKAKBJDYIKGPKAGFKYDYIZOEPSTZ
GKAGAZFJEGJAMEKPZBJMEYGAKJBAJOBXJXMAOPKYB
```

The text is written in english. Analyse the frequency of each letter and try to reconstruct the ciphertext alphabet as well as the plaintext.

2 Stream Cipher

For a stream cipher to be secure, it is crucial that a key is used only once. Otherwise, the security of the stream cipher is compromised!

Assume you have gotten knowledge of the following three ciphertexts which have been encoded using the same key:

```
1. 00001010001010000010000001100001001000011111001001101011110010 1
2. 01001010101010010010011001001101011110010101001100101001010011 1
3. 11001001101011110010101001100101001010011100001100001001000011 1
```

Additionally, you know several things about the cipher:

1. The plaintext uses characters from the ASCII table in binary format, i.e. with 7 bits per character. It can be composed of upper case characters, lower case characters and spaces.
2. The plaintext and the keystream are linked by an XOR operation.
3. For the used stream cipher, a *keyword* is used and repeated until the *keystream* has the same length as the plaintext.
4. The keystream both are composed of ASCII characters in binary representation.

Example: Consider using the keyword `UM` and the plaintext `HELLO`, then the encryption works as follows.

- The *keystream* is `UMUMU`, which is `10101011001101101010110011011010101` in binary-encoded ASCII.
- The plaintext is `10010001000101100110010011001001111` in binary-encoded ASCII.
- The XOR operation links both bit strings together and produces the ciphertext as `00111010001000001100100110010000010`.

Find out what the *keyword* and the three messages are.

Hint: Think about what happens to a character if it is XORed with a space.