CSE 484 In-Section Worksheet #4

Cryptography History

Q1. Decode the following secret word:

```
HWDUYTLWFUMD
```

Q2. What is the name of the technique used to crack substitution ciphers? Record your answer using this substitution scheme:

```
Plaintext alphabet:      ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext alphabet:     ZEBRASCDFGHIJKLMNOPQTUVWXY
```

Modern Cryptography

Q3. How many different keys are there, for a block cipher with 128 bit blocks and 256 bit keys?

Q4. How many different permutations are there over 128 bits (for a 128 bit block cipher)?

Q5. Which symmetric encryption mode would you use for the following situations? Why?

You are going to send a small one-time command to fire to your nukes.

You are living in the 1970s and want to send a long letter to your lover on ARPANET.

Q6. What is a flaw with ECB encryption?