CSE 484 In-Section Worksheet #4

Cryptography History

Q1. Decode the following secret word:

`HWDUYTLWFUMD`

`CRYPTOGRAPHY`

(Key is a right shift 5 places, go backwards in alphabet)

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
```

Substitution ciphers are broken by frequency analysis.

Encrypt by using corresponding ciphertext letter to plaintext letter (e.g. F->S, R->O).

`SOANTAKBX ZKZIXPFP`

Modern Cryptography

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

Bits are either 0 or 1, there are 256 bits: 2^{256} possible keys.

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

Possible keys from 128 bits: 2^{128}

Permutations of those generated keys: $(2^{128})!$

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.

Small message + only used once = one time pad

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

Long message = have to use a block cipher. During this time, only available block encryption standard was DES. In general, use AES if you can.

Q6. What is a flaw with ECB encryption?

Identical blocks of plaintext produce identical blocks of ciphertext- can determine the structure of the plaintext from ciphertext.

No integrity checks: can mix and match blocks and recipient would not know.