CIS 4360 Introduction to Computer Security

QUIZ 8, Fall 2011 (5 minutes only) — with answers

This quiz concerns cipher systems.

1. Ceasar's cipher is a substitution cipher in which each one of the 26 letters of the alphabet is substituted by a letter obtained by shifted it K places forward, where K is the key. For example, if the key is $K = 3$, then the word $CEASAR$ is encrypted as: $FHDVDU$ because if we shift the letters of the alphabet three places forward we get:

   $C \rightarrow D \rightarrow E \rightarrow F$
   $E \rightarrow F \rightarrow G \rightarrow H$
   $A \rightarrow B \rightarrow C \rightarrow D$
   $S \rightarrow T \rightarrow U \rightarrow V$
   $A \rightarrow B \rightarrow C \rightarrow D$ and
   $R \rightarrow S \rightarrow T \rightarrow U$

   Letters are rolled over when reaching Z. So $Y \rightarrow Z \rightarrow A \rightarrow B$.
   What is the plaintext if the ciphertext is: (*Hint:* Shift all the letters one-at-a-time)

   $$E\ W\ I\ J\ K\ P\ W\ D\ W\ Y\ G\ A\ N$$

   $$\begin{array}{cccccccccccc} F & X & J & K & L & Q & X & E & X & Z & H & B & O \\ G & Y & K & L & M & R & Y & F & Y & A & I & C & P \\ H & Z & L & M & N & S & Z & G & Z & B & J & D & Q \\ I & A & M & N & O & T & A & H & A & C & K & E & R \end{array}$$

   (The English alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ)

2. In the previous example you found the plaintext *given only the ciphertext*. This is usually the hardest task a cryptanalyst must do—of course Ceaser's cipher is a trivial cipher. We discussed "Attacks on Cryptosystems" in class and gave a special name to this "attack". What was it called?

   A ciphertext only attack.

3. The One-Time Pad.
   This is an encryption system that offers *perfect secrecy*. This means that (True or False):

   - given a plaintext, the corresponding ciphertext is random. **TRUE**
   - given a ciphertext, the corresponding plaintext is random. **FALSE**
   - the plaintext is random. **FALSE**
   - the ciphertext is random. **TRUE**

Mike Burmester