Foundations of Computer Security

Lecture 37: Cryptography

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Elementary Cryptography

Cryptography is a rich, complex subject. Our goal is to develop intuitions about:

- what are the key concepts of cryptography;
- how is it used as a tool for security;
- how effective is it in that regard.

Poe's "The Gold Bug"

The setting: In the early 1800's, a man finds a scrap of parchment on a South Carolina beach. On the parchment is a strange encoded message and a drawing of a goat's head. He wonders if the message could be directions to the location of a treasure buried by the infamous pirate Captain Kidd.

```
53++!305))6*;4826)4+)4+).;806*;48!8]60))85;1+8*:
+(;:+*8!83(88)5*!;46(;88*96*?;8)*+(;485);5*!2:*+
(;4956*2(5*-4)8]8*;4069285);)6!8)4++;1(+9;48081;
8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)
4+;161;:188;+?;
```

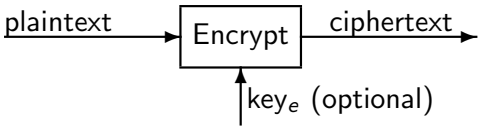

The Gold Bug

Apply your cryptanalytic skills. *How do you get started? What questions should you ask?*

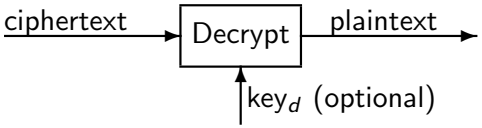
- What is the likely underlying language of the plaintext?
- What characteristics of the probable source text are relevant?
- What characteristics of the source language are relevant?
- What is the likely nature/complexity of the encryption algorithm?
- Have any transformations/compressions been applied prior to encryption?
- What else?

Encryption / Decryption

The purpose of encryption is to render the message less useful / meaningful to any eavesdropper. Conceptually, the process of encryption is quite simple:



as is the process of decryption:



Information Theory and Cryptography

Information theory informs cryptography in several ways:

- What effect does encrypting a message have on the information content of the file?
- An attempt to decrypt a message is really an attempt to recover a message from a (systematically) noisy channel.
- How can redundancy in the source give clues to the decoding process?
- Is a perfect encryption possible (i.e., one that is theoretically unbreakable)?

Lessons

- Encryption is designed to obscure the meaning of text.
- Redundancy is the enemy of secure encryption because it provides leverage to the attacker.

Next lecture: Cryptography II