Introduction to Cryptology

Relevant Definitions:

Plaintext: ***A message in plain English or any other standard language that the public can understand.***

Encryption: ***The process of disguising a message to hide its substance. Typically, this does NOT include hiding the fact that a message is sent, which is known as stenography.***

Ciphertext: ***The output of encrypting a plaintext message.***

Decryption: ***The process of recovering the plaintext from the ciphertext using a secret key that only the receiver (and maybe the sender) has.***

Cryptology: ***The science (and art) of building and analyzing different encryption-decryption methods.***

Cryptography: ***The science of building more powerful and efficient encryption techniques.***

Cryptanalysis: ***The science of discovering weaknesses in existing methods so that the plaintext can be recovered without knowledge of the key.***

Steganography: ***The science of message hiding, ie. using invisible ink, etc.***

Code: ***Substitutes words and phrases in the plaintext for numbers. No algorithm nor key is necessary, only a codebook that has an exhaustive list of every substitution.***

Cipher: ***Uses an algorithm and key to hide information.***

Our Soap Opera: One Life to Live, Days of Our Lives, … sorry just kidding, besides this class meets while both of those are on, I think!

No, really, our soap opera involves Alice and Bob (who are madly in love, though our book doesn't tell us this), and Eve (who as history tells us, is pure *evil*). Alice and Bob are sending love notes and plans back and forth, while Eve is attempting to intercept these notes and sabotage Alice and Bob's relationship. (Essentially, Eve is a homewrecker!)

In our class, we will assume that Eve only has access to the ciphertext and hasn't been able to use espionage to steal the secret key. Incidentally enough, Eve has been "eavesdropping," living up true to her name.

We will also assume that Eve has knowledge of the algorithm being used to encrypt data. This is known as *Kerckhoffs's law.*

Here are some standard ground rules for a cryptographic system laid out by Kerckhoffs in the 19th century:

1. The system should be unbreakable in practice.
2. Compromise of the system should not inconvenience the correspondents.
3. The key should be easy to remember and easy to change.
4. The cryptograms should be transmissible by telegraph.
5. The apparatus or documents should be portable and operable by a single person.
6. The system should be easy, neither requiring knowledge of a long list or rules involving mental strain.

Well the truth of the matter is that our buddy Kerckhoff lived without air conditioning, and more importantly, without a computer. The general idea behind these rules are still relevant today, but we need to make some modifications due to current technology. Here are my addendums to these rules:

1. The amount of effort to break a cryptographic system should exceed the value/lifespan of the data that is being transmitted using that system.

3. If a computer can automatically manage switching keys and "remembering" keys, then it shouldn't matter how difficult the process would be by hand.

4. Ummm, change "telegraph" to "computer."

6. Most modern cryptographic systems are quite complicated and would require insane amounts of "mental strain" to do by hand. But, this is irrelevant because once someone writes the software (or builds the hardware) following these tedious steps then the user's job becomes cake!

Here are Claude Shannon's rules:

A good cipher will involve both *confusion and diffusion.*

Confusion: *The cipher hides any local patterns. Any identifying characteristics of the language should be obscured by the cipher*

Diffusion: *The cipher mixes up different segments of the plaintext so no character is left in its original position.*

Cryptanalysis

Types of cryptanalytic attacks:

Ciphertext-only: ***Eve ONLY has a transmitted ciphertext, or multiple transmitted ciphertexts.***

Known-plaintext: ***Eve has both a plaintext and its corresponding ciphertext, or multiple pairs.***

Chosen-plaintext: ***Eve gets to choose plaintext messages and gets to see their corresponding ciphertexts.***

Clearly for the last two attacks, the goal would be to determine the key so that future messages can be deciphered, since the current messages are already known.

Historical Note

There's a rich history of cryptology which has shaped many major past events, including wars. Our text only devotes a couple pages to this, but if you are interested, a good starter book is The Code Book by Simon Singh. You can probably get it on Amazon in paperback for around 10 bucks. If you want a incredibly thorough history, then your best bet is David Kahn's The Codebreakers.

Classical and Contemporary Ciphers

Roughly speaking, classical ciphers refer to the cryptographic systems implemented by hand, whereas contemporary ciphers refer to those implemented by machine and computer.

Most classical systems utilized a combination of transposition and substitution. Transposition is the reordering of letters while substitution is substituting a symbol for a letter.

Within classical schemes, there are two main types: monoalphabetic and polyalphabetic. The former requires that one letter is always substituted with the same ciphertext symbol. The latter allows for the same plaintext letter to be substituted for by different ciphertext letters.

Page 8 of our textbook has the entire diagram of the different types of cryptographic/security systems that exist.

For right now, let's define the following:

Symmetric key: The key for encryption and decryption are the same. Alternatively, knowledge of the encryption key allows one to determine the decryption key with ease.

Public key: A public key exists that allows for encryption of a message, but does not divulge knowledge of the secret key, which the recipient uses for decryption. This is also known as asymmetric cryptographic system.