Chapter 3

Some Results From Information Theory

3.1 Levels of Security

Definition 3.1.1 *Unconditional Security*

A cryptosystem is unconditionally *secure if it cannot be broken even with infinite computational resources.*

Theorem 3.1.1 *The OTP is unconditionally secure if keys are only used once.*

3.2 Computational Security

For **all** known practical cryptosystems we have:

Definition 3.2.1 *Computational Security*

A system is "computational secure" if the ***best possible algorithm*** *for breaking it requires N operations, where N is very large and known.*

Unfortunately, **all** known practical systems are only computational secure for **known algorithms**.

Definition 3.2.2 *Relative Security*

A system is "relative secure" if its security relies on a well studied, very hard problem.

Example:

A system S is secure as long as factoring of large integers is hard (this is believed for RSA).

3.3 Cryptography and Coding

There are three basic forms of coding in modern communication systems: source coding, channel coding, and encryption. From an information theoretical and practical point of view, the three forms of coding should be applied as follows:

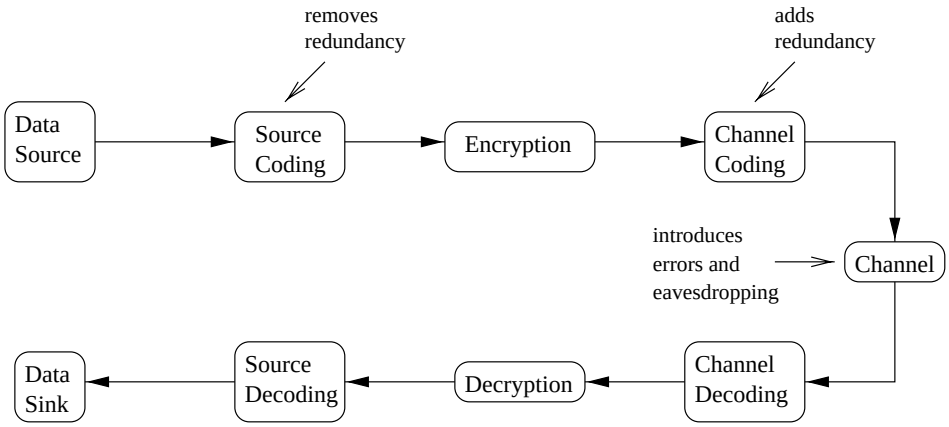

Figure 3.1: Communication coding system model

3.4 Confusion and Diffusion

According to Shannon, there are two basic approaches to encryption.

1. **Confusion** — encryption operation where the relationship between cleartext and ciphertext is obscured. Some examples are:

   (a) Shift cipher — main operation is substitution.

   (b) German Enigma (broken by Turing) — main operation is *smart* substitution.

2. **Diffusion** — encryption by spreading out the influence of one cleartext letter over many ciphertext letters. An example is:

   (a) permutations — changing the positioning of the cleartext.

Remarks:

1. Today $\rightarrow$ changing of one bit of cleartext should result on average in the change of half the output bits.
   $x_1 = 001010 \rightarrow encr. \rightarrow y_1 = 101110.$
   $x_2 = 000010 \rightarrow encr. \rightarrow y_2 = 001011.$

2. Combining confusion with diffusion is a common practice for obtaining a secure scheme. Data Encryption Standard (DES) is a good example of that.

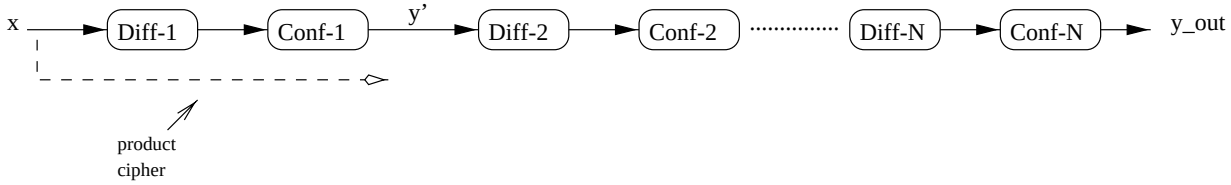

Figure 3.2: Example of combining confusion with diffusion