Introduction to Cryptology

Tutorial-05
Fundamentals of Secrecy Theory

04.04.2023, v37

Summary of security fundamentals

Shannon security theorem: Perfect Security condition is H (Z) ≥ H (X)

Unicity Distance n_u $\quad n_u = \frac{H(Z)}{r} - \frac{K}{r}$ $\quad$ Where r is the clear text redundancy $\quad r = \frac{N - H(X)}{N}$

H(Z) = Key entropy, H(x) = Information entropy, N information length, K key length

Plain Text *Padding PTP*: Clear text redundancy $r = \frac{N - H(X)}{N}$ and $n_u = \frac{K}{r}$

N Bits | L Bits padding

Clear text | H(X) | Random pattern

After PTP: $r' = r\frac{N}{L+N}$

New unicity distance: $n_u' = \frac{L+N}{N} n_u$

Problem 5-1:

A cipher encrypting an information block of 250 bits. The entropy of the information source is 150 bits.
The key length of the cipher is 64 bits.
How many cryptogram (cipher text) bits are at least necessary for an attacker to observe, in order to be theoretically capable to break the cipher.

Solution 5-1:

The minimum number of cipher text bits necessary to enable theoretically breaking the cipher is the unicity distance n_u

Where: $n_u = \frac{K}{r}$

K is the cipher key length and r the clear text redundancy.

The Information redundancy is:

$$r = \frac{n - H(X)}{N} = \frac{250 - 150}{250} = 0.40$$

The minimum number of cryptogram bits to break the cipher is

$$n_u = \frac{K}{r} = \frac{64}{0.4} = 160 \text{ bits}$$

Problem 5-2:

A cipher having a key length of 80 bits is encrypting a clear text information block of length 800 bits having an information entropy of 300 bits.

1. Compute the unicity distance of the cipher.
2. Find the new unicity distance if a random pattern of 1000 bits is appended to the information block.
3. How much Is the change in the new channel data rate?

Solution 5-2:

1. The unicity distance can be found by substituting in the formula: $n_u = \frac{K}{r}$, r is to be computed.

$$r = \frac{N - H(X)}{N} = \frac{800 - 300}{800} = 0.625 \quad , \quad n_u = \frac{K}{r} = \frac{80}{0.625} = 128 \text{ bits}$$

2. The new unicity distance $\quad n_u' = \frac{L+N}{N} n_u = \frac{800 + 1000}{800} * 128 = 288 \text{ bits}$

3. 800 useful data bits and 1000 non-useful random bits are appended to enhance security however, these additional random bits include no transmitted information.
percentage of useful data is = 800 / (800 + 1000) = 44% thus the channel data rate is reduced by 100% - 44% = **56%**

Problem 5-3:

A cipher is to be designed with a unicity distance of 2500 bits.

1. Compute the key length required for the cipher if the encrypted clear text block length is 1000 bits and clear text entropy is 500 bits.
2. Find the required data compression to reduce the key length by 20% without reducing the system security (unicity distance).
3. The unicity distance is to be increased to 3000 bits. How many random bits are to be padded to the information block to achieve the new unicity distance?

Solution 5-3:

1. The key length can be found by substituting in the relation: $n_u = \frac{K}{r}$
Where: $n_u = 2500$

and $r = \frac{N - H(X)}{N} = \frac{1000 - 500}{1000} = 0.5 \quad , \quad n_u = \frac{K}{r} \Rightarrow 2500 = \frac{K}{0.5} \Rightarrow K = 1250 \text{ bits}$

2. To reduce the key length by 20% = 1250 * 0.2 = 250 bits to become 1000 bits, and still keep the unicity distance unchanged (n_u = 2500), the new redundancy is $\quad r = \frac{K}{n_u} = \frac{1000}{2500} = 0.4$

Solution 5-3 cont.:

to find the new data length, substitute in the redundancy formula

$$r = \frac{N - H(X)}{N} \Rightarrow 0.4 = \frac{N - 500}{N} \Rightarrow N = 833 \text{ bits (data compressed to 833 bits)}$$

3.

$$n_u' = \frac{L+N}{N} n_u \Rightarrow 3000 = \frac{L + 833}{833} * 2500 \Rightarrow L = 167 \text{ random bits are to be appended to 833}$$

Problem 5-4:

A block cipher having a key length of 136 bits is encrypting a clear text having an entropy of 64 bits. The clear text block size is 256 bits.

1. Compute the unicity distance of the cipher n_u .
2. Compute the new unicity distance of the cipher if 128 random bits are appended to each clear text block. And the clear text is compressed by 50%.
3. Is the cipher theoretically breakable after this modification if the attacker can only observe 500 cipher text bits? Why?

Solution 5-4:

K = 136 Bits, H(x) = 64 Bits, N = 256 Bits, r = ?

1. Unicity distance $n_u = \frac{K}{r}$

   As $r = \frac{N - H(X)}{N} = \frac{256 - 64}{256} = 0.75 \Rightarrow n_u = \frac{K}{r} = \frac{136}{0.75} = 181 \text{ bits}$
2. The new data block length is N' = 128 (50% of the original one), entropy H(x) do not change by compression

   Therefore the new redundancy is $r' = \frac{N' + L - [H(X) + L]}{N' + L} = \frac{128 + 128 - [64 + 128]}{128 + 128} = 0.25$

   And $n_u' = \frac{K}{r'} = \frac{136}{0.25} = 544 \text{ bits}$
3. The number of observed cipher text bits is only 500 bits and is smaller than the unicity distance (544 bits). Therefore, the cipher is theoretically impossible to break.