Fundamental Concepts of Cryptography

Assignment 1

Jeremy Shade – 15182706

18/04/2016

# Affine Cipher

For to exist, a and m must be coprime. Without this, the decryption may not be possible as more than one unique value of a may exist. Following on from this, it can be shown that the decryption function is the inverse of the encryption function:

# DES

The operation of DES for ***encryption*** can be generalized to three steps:

\*Let Initial Permutation be represented by IP

Encryption and decryption of an input block share the same three steps above, only the iteration round direction is reversed due to key arrangement.

The arrangement of keys, also called the key schedule, is denoted by:

The ***decryption*** algorithm starts by inputting the cipher text as the input block:

However, since the input block is actually the output from the final step of encryption, it can be rewritten as:

Following on from step 2a of encryption, we deduce:

The right hand sides of these two assignments should be replaced with their corresponding iteration, I.e.:

with due to step 2a of encryption,

replaced by due to step 2b,

by due to the key schedule

Following this replacement yields steps 2a and 2b directly above as:

Therefore, after one round of decryption we acquire:

Thus, at the start of the next round the two half blocks are .

Following on, the next 15 rounds we will obtain:

For the final step, the two half blocks from the final round ( 16 ) are swapped, and input to the inverse of the initial permutation:

It can be seen that the output block above is the original input from step 1 of encryption.

Following the rule that for a decryption key,, and an encryption key, , that the following equation must be met for a cryptographic system:

That is,

Therefore, it has been shown that for DES that the encryption and decryption algorithms keep to this equation and holds true for .