DES暗号の仕組みについて

（情報セキュリティ　第一回レポート）

C0118005 秋本　遥基

1. はじめに

　本レポートでは暗号アルゴリズムであるDES暗号（Data Encryption Standard）の仕組みと、暗号化について考察するものである。

1. DES暗号化
   1. 平文の生成

　学籍番号の数字部分を用いて、入力値（平文）を生成する。まず、学籍番号を2進数表記に変換し、それを三回連結させる。0118005を二進数に変換すると「」である。これを三回連結させると「」となる。64bitに足りない先頭部について0埋めをし、生成された「」を入力値として扱う。また鍵に必要な64bitの数値は「」を使う。

* 1. DESの全体構造

　以下にDESの全体構造図とその中で使用される関数Fの構造図を示す（図？？？）。このように、DESの暗号の生成は転置による数値の変形とbitのシフト、排他的論理和の組み合わせによってデータの攪拌をする暗号アルゴリズムである。以降の章で具体的な作業を用いながら、その仕組みを説明する。

* 1. 転置とシフト演算による関数Fへの入力値の生成
     1. 初期転置

　図？？？の初期転置を行う。転置は図？？？、図？？？の転置表を用いて行う。転置とは以下に示すように転置表の左上から一行ごとに数字を読み込み、読み込んだ数字番目の入力bitの数値を、読み込んだ順に出力bitの一桁目から割り当てていく作業である。使用する入力値は「」であるため、出力bitは順に第58bitの「」、第50bitの「」というように定まる。

　したがって、入力bitは「」であるため、初期転置による出力bitは「」となる。

* + 1. PC1,PC2の転置

PC1,PC2では縮約転置を行う。縮約転置の操作は通常の転置と同様であるが、これは、図？？？のように8×8行列よりも小さいサイズの転置表を用いる。したがって、PC1,PC2で転置後に出力されるbit列は入力bitよりもサイズが小さくなる。

　あ

* 1. 関数Fについて
  2. （まとめ）

1. 結果
2. 考察