共通鍵暗号方式

名列番号 001　　氏名 秋元　真里絵

１．まえがき

鍵を用いる暗号方式は、暗号化、復号化に必要な鍵が同じ「共通鍵暗号方式」と鍵が異なる「公開鍵暗号方式」が存在する。当然例外もあるのだが、大体がこのふたつに二分される。秘匿性を守る為に、相手によって鍵がかわる共通鍵暗号方式より、不特定多数の相手でも鍵が同じですむ公開鍵暗号方式のほうがいいのではないか、と言う考えがあるが基本的に公開鍵暗号方式よりも共通鍵暗号方式のほうが処理時間が短いなどの利点があり、また共通鍵暗号方式と公開鍵暗号方式を合わせたハイブリット暗号方式などがある。

今回は共通鍵暗号方式の中でも、DES について取り組んだ。

２．研究課題

DES とは Feistel ネットワーク構造を用いた共通鍵暗号方式で、暗号化と復号化では鍵から生成されたサブ鍵の再生が逆順ということを除けば、全く同じアルゴリズムを用いる。　手順は、初期転置→Feistel ネットワークによる暗号化、または復号化→最終転置となる。

また暗号化、復号化にとって大変重要となる考え方が$(A \oplus B) \oplus B = A$であり、効率よく複雑化ができるため DES のみならず共通鍵暗号方式で多く用いられる考え方である。

３．研究方法

DES のプログラムを実際に組み、暗号化、復号化される様子を観察する。また、DES に使われている各関数について正しい動きをしているか手計算で確認。

方法はまず、単純な入力をし次に複雑な入力をし整合性を確かめる。

４．実験結果と考察

ある平文の実行結果である。

平文：123456789abcdef0

暗号文:40c9364be2e0c4a2

[過程] (fp は初期転置の事)

	暗号化	復号化
fp	ccff6600f0aa7855	7b04440af2b40a9c
1	d38e8554f0aa7855	c73f1a07f2b40a9c
2	83f7a8add38e8554	8fa45c25c73f1a07
3	917232b883f7a8ad	d205b2828fa45c25
4	54e2efa4917232b8	5554de13d205b282
5	b2e64c5c54e2efa4	427ffe435554de13
6	abb7640eb2e64c5c	58a01c54427ffe43
7	f289fb36abb7640e	fa4186af58a01c54
8	fa4186aff289fb36	f289fb36fa4186af
9	58a01c54fa4186af	abb7640ef289fb36
10	427ffe4358a01c54	b2e64c5cabb7640e
11	5554de13427ffe43	54e2efa4b2e64c5c
12	d205b2825554de13	917232b854e2efa4
13	8fa45c25d205b282	83f7a8ad917232b8
14	c73f1a078fa45c25	d38e855483f7a8ad
15	f2b40a9cc73f1a07	f0aa7855d38e8554
16	7b04440af2b40a9c	ccff6600f0aa7855

以上のように平文とは全く関係ないように変化し続けているのがわかる。また、暗号化復号化の手順では右半分が逆順位になっているのがわかる。

５．まとめ・感想

結果確認作業やプログラムの修正に思いのほか時間がかかった。また、以上を参考に自作の暗号を作成する時間が無かったことが残念である。

６．参考文献

情報セキュリティの理論と技術 - 暗号理論から IC カードの耐タンパー技術まで［著者］神永 正博 , 渡邊 高志