DES と AES の比較

青野麻奈　(指導教員：萩田真理子)

1　研究背景

DES は 1976 年に標準暗号として採用され，ブロック暗号の代表的な規格として広く使われてきた．しかし 1997 年アメリカ合衆国において，急速な計算機の処理速度の上昇によって DES がもはや安全ではなくなってきたことを理由に，新しい規格として AES(Advanced Encryption Standard) が世界規模で公募された．そして 2001 年 3 月，J.Daemen と V.Rijmen が提案した Rijndael が AES として採択され公表された．以降，AES はアメリカ合衆国のみだけでなく，欧州の暗号規格 NESSIE や日本の暗号規格 CRYPTREC にも採用され，今日の共有鍵暗号方式の代表的な規格の一つとして利用されており，新たな共有鍵暗号方式の規格を提案する際の速度や安全性の評価基準としても利用されている．本研究では，ブロック暗号の標準として長く使われてきた DES と，その後継である AES の安全性を評価・比較する．

2　DES(Data Encryption Standard)

2.1　仕様

ブロック長 64bit
鍵長 64bit(ただし 8bit はパリティビット)
ラウンド数 16

2.2　暗号化アルゴリズム

DES の暗号化アルゴリズムは以下の通り．

1. InitialPermutation(IP) によりビット置換を行う．
2. Feistel 構造部分を 16 回繰り返す．(最終ラウンドのみ左右の入れ替えを行わない)

   $(L_i, R_i) = (R_{i-1}, L_{i-1} \bigoplus f(K_i, R_{i-1}))$
3. FinalPermutation(FP) によりビット置換を行う．

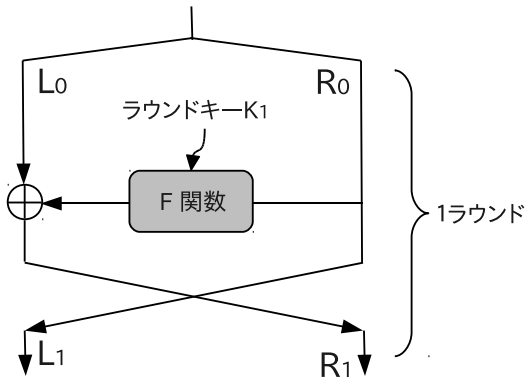

図 1: DES・Feistel 構造部分の流れ

3　AES(Advanced Encryption Standard)

3.1　仕様

ブロック長 128bit，192bit，256bit の中から選択可能
鍵長 128bit，192bit，256bit の中から選択可能
ラウンド数 鍵長に依存．鍵長 128bit：10 回，192bit：12 回，256bit：14 回

本研究ではブロック長 128bit，鍵長 128bit を使用する．

3.2　暗号化アルゴリズム

AES(ブロック長 128bit) の暗号化アルゴリズムは以下の通り．

1. 入力された平文を 8bit 毎に区切り，4 × 4 マス (state) に振り分ける．
2. 入力された鍵を KeyExpansion 関数を用いて【規定ラウンド数 +1】(11) 個に拡張．
3. state に対して AddRoundKey 変換を施す．
4. state に対し，SubByte 変換，ShiftRow 変換，MixColumn 変換，AddRoundKey 変換を【規定ラウンド数 −1】(9) 回繰り返し行う．
5. 最終ラウンドのみ，SubByte 変換，ShiftRow 変換，AddRoundKey 変換だけを行う．

4　評価方法と結果

4.1　安全性の高い暗号の条件

安全性の高い暗号の条件の一つとして，類似性の高い平文の集合が類似性の低い暗号文の集合へと変換されることが挙げられる．これは，類似した平文から類似した暗号文が生成されてしまうと，解読したい暗号文に類似した暗号文を用いて平文を推測されてしまう恐れがあるからである．従って，偏った平文の集合から生成された暗号文の集合に偏りがおきない必要がある．この条件を満たしているかについて各暗号の評価を行った．

4.2　評価方法

各暗号文の 1 のビットの数を数え，その分布と確率による期待値の分布を比較．ただし AES は暗号文 128bit 中の前半 64bit のみ 1 の数を数える．評価条件は以下の通り．

平文空間 DES は 64bit 中 1 のビットが 2 つだけの類似した平文の集合．AES は 128bit のうちの前半 64bit 中 1 のビットが 2 つだけの類似した平文の集合．ともに 2 つの 1 ビット以外はすべて 0 ビットとする．

鍵 0(全て 0 のビットのみ)

ラウンド数 1〜規定ラウンドまで観測

4.3 結果

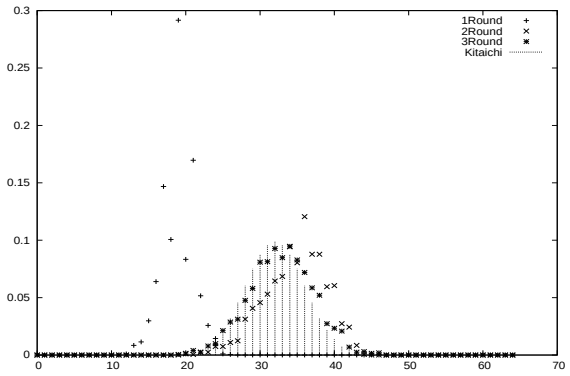

図 2: DES を 1,2,3 ラウンド行った時の分布

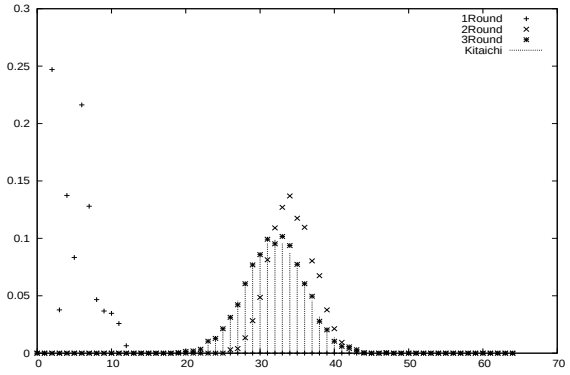

図 3: AES を 1,2,3 ラウンド行った時の分布

どちらも期待値の確率の分布と比較すると，2 ラウンドまでは偏りが見られるが，3 ラウンド操作すると期待値と変わらない分布を示している．そこで，同じ条件において χ^2 検定を用いてより精密な評価を行った．

$$\chi^2 = \sum_{i=1}^{m} \frac{(O_i - E_i)^2}{E_i}$$

O_i : 観測度数　E_i : 期待度数　m : グループ数

上記によって得られた χ^2 値を表 1 に示す．m=3 としたので自由度は 2，有意水準は 0.01 とする．暗号化した結果の分布が，確率による期待値の分布と同じ分布を示すとすると，χ^2 値が 9.210 より大きくなる可能性は，1 %以下である．

Round	1	2	3	4
DES	3679.0	789.34	78.007	0.52115
AES	3679.0	684.69	0.28326	0.44712

表 1: DES・AES の χ^2 値

表 1 を見ると，どちらもラウンドを進めるごとに偏りがなくなっていくことがわかる．1，2 ラウンドの場合はどちらも χ^2 検定において棄却されるが，3 ラウンドでは DES のみが棄却された．つまり，図 2 では DES の 3 ラウンドも期待値と同様の分布をしているように見えたが，実際は結果に偏りがあることがわかる．

以上より DES より AES の方が乱数性が高いことがわかった．

5 DES の各操作に対する評価

先行研究により，AES の安全性は 4 つの変換を組み合わせることに起因しており，全ての変換が不可欠であることがわかっている．

そこで本研究では，DES においてどの変換が重要なのか検証した．

5.1 評価方法

前述の DES アルゴリズムにおいて，IP・FP 変換，f 関数，Feistel 部の左右入替の 3 つの操作のうち，どれか 1 つを除去して暗号化を行い，暗号文の 1 のビットの数を数える．

平文空間 64bit 中 1 のビットが 2 つだけの類似した平文の集合

鍵 0(全て 0 のビットのみ)

ラウンド数 1〜規定ラウンドまで観測

5.2 結果

IP・FP 変換はどちらも並び替えるだけの変換である為，暗号文の 1 のビット数には影響しない．f 関数を除去すると，3 ラウンド行うごとに，元の平文と同じ出力になる．左右の入替を行わないと，同じビット列に対して排他的論理和を 2 回行う為，2 ラウンドごとに元の平文と同じ出力になる．

今回の評価方法においては，IP・FP 変換は暗号化に影響を及ぼさないことがわかった．しかし f 関数と左右入替を除去すると，2 または 3 ラウンドごとに平文と同じ暗号文が生成されてしまう．よって DES においてこれら 2 変換は不可欠な操作であるとわかった．

6 まとめと今後の課題

本研究では，3 ラウンドで χ^2 検定を行った結果，DES のみが棄却された．つまり，AES のほうが DES よりも 1 ラウンドの変換での乱数性が高いことを示している．これは 1 の研究背景で述べた，AES は DES の後継であるという事実とも合致する．また DES は Feistel 構造を崩すと，安全な暗号文を生成出来なくなることもわかった．

今回は鍵をすべて 0 として暗号化を行ったが，今後は鍵を変化させるなど，その他の条件でも評価・比較を行っていきたい．

参考文献

[1] Johannes A. Buchmann, ”INTRODUCTION TO CRYPTOGRAPHY”, Springer, 2000.

[2] 草間時武, ”統計学”, サイエンス社, 1975.