暗号攻撃

Cracking Against a Cryptography

窪田 耕明 , 日下部 明（知的システムデザイン研究室）
Koumei KUBOTA , Akira KUSAKABE（Intelligent Systems Design Laboratory）

Abstract There are two typical type of cryptosystem which is DES(Data Encryption Standard) and RSA(Rivest,Shamir, Adelman).This paper explains these two first then this paper introduces GCC(Gao's Chaos Cryptosystem) that has been replaced DES and RSA.And this paper also explains cracking against these cryptography.

1　暗号とは

暗号 (cryptography) とは，データを部外者に読み取れないようにする方法の総称であり，また電話回線，衛星，コンピュータのいずれを問わず，大規模な通信回線網を通じて伝送される情報を保護する為の唯一の既知の実用的方法でもある．

2　現在主流の暗号

現代の暗号は DES(Data Encryption Standard) に代表された慣用暗号方式と RSA(Rivest,Shamir, Adelman の３人) に代表された公開鍵暗号方式に大別できる．DES は，数十ビット以上の比較的長いデータブロックごとに暗号化・復号を行う方式である．RSA は，非常に大きな２つの素数の積である合成数の素因数分解が極めて難しいことを巧みに利用して公開鍵暗号を実現した方式である．

RSA は DES よりも強度の強い暗号方式として誕生した．それでもなお，RSA と DES は併用されているのである．その理由は，DES のほうが RSA よりも処理速度が速く，サイズの大きいメッセージの処理に適しているからである．つまり RSA はより安全性が強まったが負荷が重いというのに対して，DES は負荷は軽いが安全性については RSA にやや劣っているということである．

DES や RSA ではキーを長くすればより安全になるが，長くするほど複合化するときに時間がかかってしまう．そこでキーが短くても DES や RSA よりも安全性の高く，さらにキーが長くてもそれほど時間のかからない GCC（Gao's Chaos Cryptosystem) という新たな暗号方式を紹介する．

3　GCC 暗号

GCC 暗号は以下の４つのようなカオスの特性を利用している．

- 奇妙なアトラクタ (strang attractor) があるが，軌道は不安定で，周期性はない
- 初期値に敏感な性質 (sensitive dependence on initial condition) がある
- 「引き伸ばし」と「折り畳み」があり，予測できない
- 一方向性を有する

GCC は，ストリーム型，共通キー方式，デジタル式カオス暗号方式である．その仕組みは，図 1 に示すとおり，平分をまずカオス信号により暗号化し，送られた暗号をまたカオス信号により複合化するというものである．

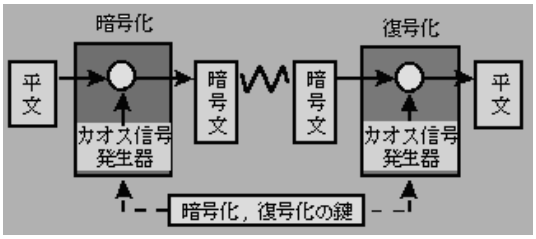

図 1: GCC カオス暗号の仕組み

4　GCC の特徴

GCC の特徴として，その一つに超高速というのが挙げられる．ブロック型の暗号ならば平文信号をブ

ロック単位で何回も変換すること（DESで１６回）が必要なので時間が非常にかかることに対して，GCCはカオス信号を１回だけ平文信号に付加すること，かつ，カオス関数の計算が簡単なので極めて速い．

また，現在では最強の安全強度であるというのも特徴の一つである．GCCはカオスの特性を利用した最新の暗号であるので，暗号化キーを知らない限り現在使われている線形攻撃法，差分攻撃法などの解読手法で暗号文を解読することは不可能である．また0,1バランス分析によりGCCで暗号化された文書の0,1頻度はほぼ0.5：0.5となり,原文の統計的性質は完全に隠されたので統計分析攻撃にも非常に強い．またGCCはカオス信号を一方向の変換,カオス関数自身の「一方向性」,キー処理プロセッサの一方向性という多重構造になっているので,キーを割り出すことは不可能である．

5　暗号攻撃

暗号は部外者にデータを読み取れないようにする方法であると1節で述べたが，現実にはさまざまな所で部外者がデータを入手している．つまり暗号を何らかの手段で解読しているのである．ここではその手段をいくつか説明する．

5.1　片方向性関数に対する攻撃

例えば，RSAなどの公開鍵暗号方式は片方向性関数を利用したものである．片方向性関数とは，ある一方向の処理が反対方向の処理よりもはるかに容易な数学的関数のことを言う．つまりRSAで言うと，２つの非常に大きな素数から合成数（２つの素数の積）を求めるのは簡単だが，合成数から２つの素数を求めるのが非常に困難という性質を利用しているのである．RSAの安全性は，因数分解が困難な点に依存しているので，この非常に困難な素因数分解ができてしまえば，RSA暗号方式は，簡単に解けてしまうのである.

5.2　全数探索法

現在主流の暗号であるDESやRSAに対する暗号攻撃の中で，最もよく行われているシンプルな攻撃法が全数探索攻撃法（brute force）である．これはすべての可能な鍵を試してみることである．このタイプの攻撃はいつでも発生する可能性があり，それを防ぐことは不可能である．よってこの攻撃を防ぐためには，コストが時間的，金銭的に膨大なものとなり，誰もそれを実行してみようと思わないようにさせることである．平均的には（鍵の全数×一回の復号化時間÷2）の時間があれば鍵を求めることができる．近年コンピュータの速度が上がってきているのに伴って，総当たりにかかる時間が減少し，徐々に暗号が弱くなってきている．例えばアメリカのRSA Data Security社が開催したDES暗号の解読コンテスト「DES Challenge III」が22時間15分で破られたというのがある． 解読に成功したのは，世界中のインターネットユーザーを集めるプロジェクト「Distributed.Net」と「Electronic Frontier Foundation's(EFF)」だった． 両者はインターネットに接続された10万台近いパソコンに処理を分散し並列して解読を進めており，毎秒2,450億のキーをチェックしていた．なお，同社が開催している暗号破りコンテストでは，RC5方式のうち暗号鍵の長さが40, 48, 56 bitのものと，DES方式のものは既に終了している．つまり全数探索法は，処理能力の向上によって強大な威力の攻撃法にも成り得るということである．

6　まとめ

コンピュータの高速化に伴って，多少キーを長くしても複合化に時間がかからなくなってきた．さらにより強度の高いGCCなどの暗号方式もこれから出てくるであろう．しかしどんなにキーを長くしたり，強度を高めたとしてもそれは，全数探索法にかかると必ず解読されてしまうという事実からは，逃げることができないのである．

参考文献

[1] 今井秀樹『暗号のおはなし』（日本規格協会，1993）

[2] RSA LABORATORIES『最新暗号化技術に関するRSAのFAQ』（http://www.rsa-japan.co.jp/faq/faq_fdl.html，1993）

[3] IISI株式会社国際情報科学研究所『GCCカオス暗号』（http://www.iisi.co.jp/reserch/GCC-gaiyou.htm，1997）