ストリーム暗号

山中 亮典，伊藤 博高
Ryosuke YAMANAKA，Hirotaka ITO

1　はじめに

近年，情報化社会の発展が進むにつれて，電子商取引や電子化された行政サービスなど，重要なデータをインターネット上でやり取りする機会が増加してきている．それに伴って，電子化された情報の漏洩や，データの改竄などの問題が生じてきている．そこで，データの安全性を保障するため，暗号技術が重要視されている．近年の情報の大規模化，通信の高速化に伴い，暗号技術の中でも高速処理に優れるストリーム暗号が注目されている．

2　暗号技術

暗号とは，鍵と呼ばれる，第 3 者が知らない情報を用いて，第 3 者に内容を知られないようにするための技術である．

送信者が受信者に送りたいそのままの情報を平文という．そして，第 3 者に見られても内容が分からないように平文を変換するプロセスが暗号化である．暗号化用の鍵で暗号化された平文は暗号文と呼ばれ，暗号文を平文に戻す作業を復号と呼ぶ．また，暗号化および復号を行うための手順をアルゴリズムと呼ぶ．古くから使われており，代表的なストリーム暗号であるシーザー暗号の暗号化の流れを Fig. 1 に示す．

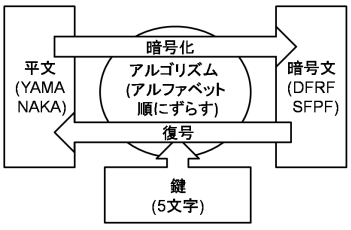

Fig.1　シーザー暗号の流れ [参考文献 1) より引用]

Fig. 1 のように，「YAMANAKA」という言葉をアルファベット順に 5 文字後ろの文字に変換するというアルゴリズムで暗号化する場合を考える．この時，平文は「YAMANAKA」であり，アルゴリズムは「平文をそれぞれアルファベット順に鍵の文字数分後ろにずらす」，鍵は「5 文字」，暗号文は「DFRFSFPF」ということになる．

3　ストリーム暗号

3.1　ストリーム暗号とは

ストリームとはデータの流れであり，ストリーム暗号は，入力されたデータの先頭から末尾までを，ビットもしくはバイト単位で逐次暗号化を行う方式である．

一般的には，疑似乱数を生成する際に用いるアルゴリズムは大きく 2 つの段階に区別できる．1 つは疑似乱数生成器内の内部状態を初期化する鍵スケジューリングアルゴリズム（KSA），もう 1 つは内部状態を更新しながらキーストリームを生成する疑似乱数生成アルゴリズム（PRGA）である．暗号化に用いる疑似乱数は一度使用すると二度と再利用してはいけないので，KSA では鍵の他に毎回異なる初期化ベクトル（IV）という値を与えることで，生成する疑似乱数を毎回異なるものにしている．Fig. 2 のように，鍵と IV を KSA に入れて内部状態を初期化し，PRGA で内部状態を更新しながらキーストリームを生成するのが基本的なストリーム暗号の疑似乱数生成方法である．生成したキーストリームと平文もしくは暗号文の排他的論理和をとることで暗号化および復号を行う．

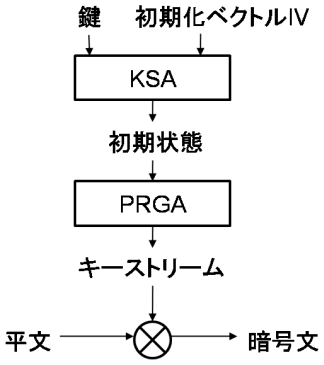

Fig.2　ストリーム暗号の流れ [参考文献 1) より引用]

3.2　ストリーム暗号の用途

ストリーム暗号は平文のサイズに依存しないため，キーストリームを先行して生成できるので，待ち時間が少なく高速である．そのため，大容量のデータをやり取りする際に適している．また，常に平文サイズの大きさと暗号文サイズの大きさが同じとなるので，平文がいつ何バイト発生するか不確定なアプリケーションの暗号方式として用いられている．高速であることおよびデータサイズが増加しないことは，主に音声データや無線通信などに利用する場合に大きなメリットとなる．現在最も利用されているストリーム暗号は，主に無線通信に用いられる RC4 である．

4　RC4

4.1　RC4 の概要

RC4 は現在主として利用されているストリーム暗号方式のアルゴリズムである．RC4 の特徴として非常に短い

コードで記述できる点およびソフトウェア上で非常に高速に動作する点が挙げられる．サーバ・ブラウザ間通信の標準プロトコルである SSL（Secure Sockets Layer）/TLS（Transport Layer Security）や無線 LAN 用のプロトコルである WEP（Wired Equivalent Privacy），その後継である WPA（Wi-Fi Protected Access）など，様々な標準規格に採用されている [2]．

4.2 RC4 の構造

RC4 は 8 ビットから 2048 ビットの間から鍵長を選択できるが，鍵長の安全な長さとしては 128 ビット以上が基本となっている．RC4 の内部状態は 2^n 個の要素を持つ配列と 2 個のカウンタから構成されており，要素とポインタはそれぞれ n ビットの変数であり，一般的に 8 ビットが採用される．

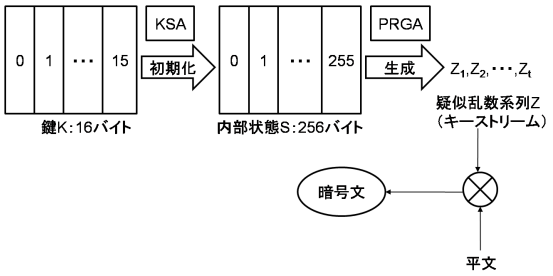

Fig.3　一般的な RC4 の構造 [参考文献 [3] より引用]

したがって，RC4 は内部状態として Fig. 3 のように 1 バイトの配列を 256 個有している．そして，2 個のカウンタを用いて内部状態の配列要素を入れ替えていくのが RC4 の PRGA になっている．内部状態を S（S_0〜S_{255}）カウンタを i, j とすると，ランダムなバイト Z を生成するためには，以下を実行する．

1. $i = (i + 1) \bmod 256$
2. $j = (j + S_i) \bmod 256$
3. S_iと S_jを入れ替える
4. $t = (S_i + S_j) \bmod 256$
5. $Z = S_t$

また，内部状態の初期化は以下のように行う．

1. $S_0 = 0, S_1 = 1, \cdots, S_{255} = 255$ のように内部状態 S をインデックスで埋める．
2. 内部状態 S と同じ長さの別の配列 K を鍵で埋める．
3. $j = 0$
4. i = 0〜255 に対して
   $j = (j + S_i + K_i) \bmod 256$
   S_iと S_jを入れ替える

このように，RC4 の KSA, PRGA はスワップ処理を中心としたアルゴリズムであるので，共に非常に短いコードで記述できるという特徴がある．また他のストリーム暗号同様，KSA に秘密鍵を入力することで内部状態を初期化し，PRGA に初期化した内部状態を入力することでキーストリームを生成する．

そしてこのキーストリームと平文および暗号文との排他的論理和をとることで，RC4 の暗号化および復号は完了する．

5 無線通信

5.1 無線通信における暗号化

無線通信とは，ケーブルを使わずに電波を用いた通信である．無線通信にはケーブルに縛られないというメリットがあるが，電波が不必要なところまで届いてしまうというデメリットも存在する．無線通信の代表である無線 LAN では，50〜100 m ほど電波が届いてしまう．何のセキュリティも施していない無線 LAN を使っていると以下の 2 つの問題が発生することになる．

- 外部から無線 LAN に不正侵入される
- 通信内容が第三者に漏洩する

前者に対しては，MAC アドレスによる接続拒否で対応している．しかし，MAC アドレスだけでは，後者の問題に対処できない．そこで，通信を傍受されても，その内容が分からないようにする暗号技術が用いられている．それが，無線 LAN 用のプロトコルの WEP である．

5.2 WEP

WEP には，暗号化方式として RC4 が採用されていて，暗号化に用いる鍵のことを WEP キーという．WEP の最初の方式は，40-bit WEP と呼ばれ，40 ビットの WEP キーを用いる規格であったが，より強固なセキュリティを求める声に応える形で 104 ビットまで拡張された．WEP では, Fig. 4 のように 24 ビットの IV と WEP キーをつなげて平文を暗号化する．

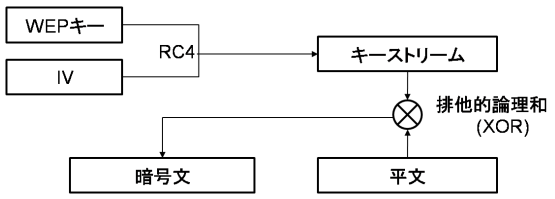

Fig.4　WEP のアルゴリズム [参考文献 [3] より引用]

しかし 2001 年, 特定の IV を用いた際に, キーストリームに WEP キーの情報が漏洩することが発見され，WEP の脆弱性が指摘された．WEP キーは固定の値なので, 暗号化の際に変更できるパラメータが IV の 24 ビットしかないことが原因だった．また 2008 年には，わずか 10 秒で WEP が破られるという発表がなされ，もはや WEP では安全な通信は全く期待できないことが証明された．

5.3 WPA

WEP の脆弱性が発見された翌年の 2002 年，WEP を改善した新たな暗号技術である WPA が提案された．WPA は WEP の後継であり，暗号化に用いる鍵を WPA キーという．WPA では，WPA キーを 104 ビット，IV

を 48 ビットに変更した．初期化ベクトルを増やすことによって生成する疑似乱数の幅を広げ，根本的な暗号強度を上げることに成功した．また WPA では，TKIP（Temporal Key Integrity Protocol）と呼ばれる暗号化プロトコルを使用している．

TKIP では, WEP と同じくストリーム暗号である RC4 のアルゴリズムを採用している．しかし，WEP での問題を改善するため，WEP では固定の値であった暗号キー（WEP キー）を一定時間毎に変更できるようにしている．これによって暗号キーを推測することが難しくなり，WEP を解読した手法では WPA が破られることはない．

しかし，TKIP はキーを頻繁に切り替えるメカニズムをソフトウェアで実装しているため，処理速度が低下してしまっている．それではストリーム暗号を用いる意味が無くなってしまう恐れがある．そのため，安全で高速なストリーム暗号が必要になってきている．近年，新たなストリーム暗号を選ぶプロジェクトが立ち上げられ，そこで選ばれたストリーム暗号が期待を集めている．

6　eSTREAM

2004 年に情報セキュリティ研究者間の連携をより密にするため，ECRYPT（European Network of Excellence for Cryptology）が設立され，次世代のストリーム暗号を選定するための「eSTREAM プロジェクト」が立ち上げられた．eSTREAM プロジェクトは広くストリーム暗号のアルゴリズムを公募し，集まった暗号に対して世界中の研究者が評価および選定を行った．そして 2008 年に選定を終了し，最終的に 7 種類のストリーム暗号が eSTREAM 暗号として選定されている．

既にデンマークのセキュリティ会社である Cryptico から eSTREAM 暗号の一つである Rabbit という暗号アルゴリズムを用いた Crypticore という暗号技術が提案されている．Crypticore を採用したセキュリティソフト，SSH Technica は以前のバージョンより 2〜8 倍の速度を実現している [4]．

7　まとめと今後の展望

ストリーム暗号は，処理速度に優れた暗号方式である．平文をビットおよびバイト単位で扱うことにより，平文のサイズに依存しない処理が実行でき，高速処理を実現している．現在無線通信における暗号化アルゴリズムとして利用されている WEP にもストリーム暗号である RC4 が採用されている．しかし WEP には脆弱性が存在し，その脆弱性を補うための暗号化アルゴリズム WPA が開発された．WPA において，WEP での脆弱性は克服されたが，処理速度が低下してしまい，ストリーム暗号のメリットが発揮されなくなってしまった．そこで近年では，より性能の良いストリーム暗号を選出し，暗号技術の新たな基準として利用しようとする動きが広まっている．選出されたストリーム暗号は，次世代の暗号化技術として期待されている．

世界中で進行する情報量の増大は，今後も拡大していくと考えられる．それに伴い，インターネット上で扱うデータの重要性も上がっていくだろう．その中で，高速処理に優れるストリーム暗号は今まで以上に必要とされ，様々なセキュリティソフトに用いられていくのではないだろうか．

参考文献

1) Sbi net system. http://dev.sbins.co.jp/.
2) 森井昌克, 寺村亮一．ストリーム暗号の現状と課題. pp. pp69–70, 2008.
3) Think it. http://thinkit.jp/.
4) japan.internet.com. http://japan.internet.com.