# Jump・Stop 方式を用いた M 系列を利用する暗号装置に関する研究

志方　泰*　　杉本雅彦**

## 1. 緒言

情報化社会といわれる現代に於いては，国家より個人のレベルに至るまであらゆる範囲のプライバシーを守ることが必然性を帯びる様になった。

特に情報ネットワークの拡大，高度化に伴い，或る種の目的を持って盗聴，改ざん，介入，不正利使用等による犯罪が行われてきている。そのため，そこに携わっている人々の間に防犯上の深刻な問題が生じ，情報に対するセキュリティー対策が必要不可欠な要素となった。この目的に対しては暗号の使用が一般的であり，特に回線用としては公開鍵暗号方式が著名である。

筆者らは，主としてパソコン通信を対象とした，通信内容の暗号化について研究を行った。その結果，ソフトウェア及び操作が簡単でかつ実用上十分な暗号強度を有するシステムについてほぼ満足すべき結果が得られたのでここに発表する次第である。

## 2. 本装置の必要性

暗号を歴史的に時代区分すると，理論的な研究が組織的に行われていなかった原始時代，行われていたが手作業で暗号を作成していた古典時代，機械及び電気式作成方法となった近代，電子化された現代，の四期になると言えよう。

日本に於ける暗号は，武田信玄が用いたといわれる“みかたそつよし”を Y7～Y1 に，“てきはほろふる”を X7～X1 に対応させ，みて＝Y7X1＝イ，かて＝Y6X1＝ロ…としてイロハ 48 文字とン，を暗号化した表が知られているが，それ以後本格的と言える暗号を用いたことは知られていない。明治維新以後設立された陸・海軍においても研究は余り行われなかったが，大正 10 年外務省電信課分室に陸・海軍，外務省，逓信省が連合して暗号研究会を発足させた。しかして暗号の維新化といわれるのが，ヤン・コワレスキーによって陸・海軍の関係者に大正末期に行われた講習であり，これが，近代暗号の幕開けとなったといわれている。現代暗号は乱数を使用することが常識となっているが，日本では昭和 11 年に初めて乱数式が原久中尉（当時）に依って用いられた。第 2 次大戦中においても 4 桁の数字（0000～9999）が書かれたカードを 1 万枚用意し，アトランダムに抽出して，乱数表を作成したと直接，原氏より御伺いした。

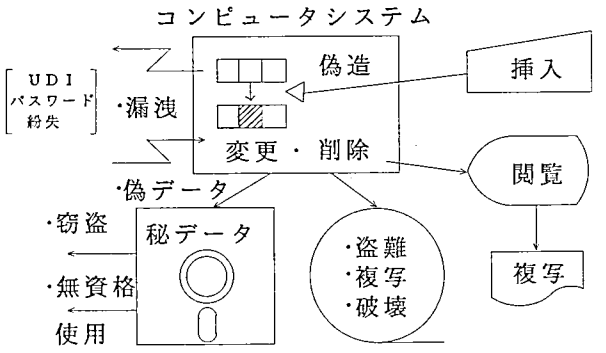
一方，乱数の補給作業能率の点から暗号機が発明され，ドイツのエニグマ，クリハなどもよく知られているが，機械式としては，クリプトテクニック（C－36），クリプトグラファー（C－52），同（CX－52），－何れも HagclimCrypt 社－，及び米陸軍で使用された M－209 が同一系列として，最も著名である[1]。乱数を，クリプトテクニックのみは算術和（mod26）で合成するが他の三種は，集合和（mod26）で合成する。キーホイー

＊　理工学部電気工学科　教授
＊＊　理工学部電気工学科　大学院生

ルは何れも6個用いられ，1クリックずつ進行するがCX－52のみは，乱数によって，0～4クリックジャンプ或いはストップする機構となっている。

さらに、テレタイプ暗号機が用いられて来た。そのため，スミス・コロナ（米），オリベッティ（伊）等のタイプライタメーカーも製造を始めた。これからは，軍，外務，国務関係に用いられることが多く，民間では商社などでも余り使用されなかった。その後，エレクトロニクス，特にコンピュータの発達に伴い処理速度が飛躍的に向上し，従来の機械暗号ではその強度に不安が生じ，一方では伝送速度の面でも追随できなくなって来た。そのため新たに電子式の暗号が考えられ，公開鍵暗号方式がDES（Data Encription Standard）として，1977年7月米国連邦規格となった。

以来，急速なコンピュータシステム及びネットワークの発展に伴い，処理したデータをメモリやその周辺装置にデータベースとして長期間にわたって記録保存したり，あるいは一時記憶の後にネットワークを通して送受信することが多くなって来た。このため，暗号を通信保護の手段のみでなく，記憶データの保護手段としても採用する考え方が次第に常識となって来た。その主な理由は，ネットワークシステムに於いて図－1に示すような第三者の多種多様な介入により，データの安全管理が危険にさらされて来だしたからである。たとえば，メッセージに暗号化を施さなければ，高速データ通信といえども盗聴，傍受などにより情報を知らされる恐れがあり，さらに積極的な行為として為電などの直接的な手段で介入し，送受信データの部分的な変更な更新，追加を強いられた思いがけない被害を受けることもある。




**図－1　コンピュータデータに対する脅威**

また，コンピュータシステム内部においては重要データを端末からのぞき見（browsing）したり，漏洩や挿入，変更，複写，削除，あるいは故意の破壊などの工作が可能であろう。利用者番号（user identification number: UID）と暗証番号（password）による現在の認証システムでも，その紛失，盗聴などにより，単に不正利使用されるばかりでなく，ファイル改ざん，その他の犯罪行為が発生しつつある。この様な各種の脅威から大切なデータを保護するには，データそのものを暗号化する必要がある[2]。要するにあらゆるレベルで犯罪や事故を防止する要求があり，個人のレベルでも同様に信書の秘密保持などの問題があるので，個人用暗号装置の必要が生じて来たのが開発の所以である。

本研究では，通信内容の保護についておこなった。この他にも通信内容の保護と同様に送受信者名や通信発生時刻に関する情報の保護などについて送受信者追跡の不可能な通信プロトコル[3]なども発表されているが，これらのことは，ここでは対象外なので考慮にいれていない。

### 3. システムの概要

大量の情報を暗号化するには，乱数を使うことが多い[4]。前述の暗号機が即ち乱数発生機である。現在用いられている2進数の方式の元祖とも言うべきバーナム（Vernam）方式の暗号は，平文の文字列を2進コードに直したものに2進の乱数（鍵）を加える（排他的論理和をとる）だけというものであるが，理論的にも絶対に解読できない[5]様にするには1度使用した乱数列は2度と使わないようにしなければならないので，乱数を常に補給し続ける必要が生じる。乱数の供給源としては，抵抗，半導体，放電管から生じる雑音や，放射線，宇宙線などが用いられる。この方法は乱数の補給と，端末への供給に手間がかかるため，コストより機密性がきわめて重視される場合に適している。製品としては放電管のノイズを利用して，毎秒400字（2000ボー）程度のスピードで乱数を作り出し5単位の鑽孔テープとして出力する機械（Cripto A.G .ZG−543）が約30年前に既に市販されている。

しかし，運用上の問題その他幅広い実用性という観点からは，理論的には，解読は可能であっても，そのための時間と手間と費用が膨大であるため，現実的には解読不可能，あるいは，ダイヤル金庫と同じように一定の時間さえ解読されなければ良い，という考え方で暗号装置がつくられている。コンピュータ・メーカーが発売している暗号装置は，大部分がこの方式である。

この場合は，有限の擬似乱数列を電子的（機械的，電気的に付する意味）に作り出し，任意の箇所から使う方法が一般的である。もちろん，有限とはいっても，乱数の量が十分でないと，繰り返し使用頻度が高くなって，暗号の強度は低下するので運用上の注意が必要である。この方式では，送信側と受信側の乱数発生装置を同期させて，同一乱数列を発生させ，簡便に暗号化，翻訳ができるので，あらかじめ乱数を配っておく必要はない。

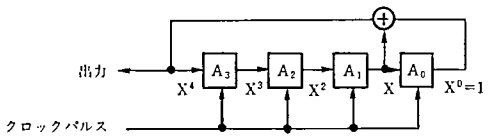
本暗号装置で用いられた乱数の発生は，フィードバックシフトレジスター方式であるが，単なる循環レジスターでは，nビットの循環数列が作られるのみであるから，実用とするには，長大なレジスター回路を要する。そこで，出力以外の部分からもフィードバック回路を分岐させ，ここからでてくる数字と出力の数字（いずれも0か1）の排他的論理和を求め、その結果を入力に帰還すれば同じ数のレジスターで，より長周期の乱数列が作成できる。

循環レジスターの回路を，次のように

$$F(x)=x^n+ax^{n-1}+bx^{n-2}+\cdots\cdots+1$$

の多項式とし，分岐点の係数を1，非分岐点の係数を0とする。この多項式が既約となる。換言すれば，因数分解できないものになるよう分岐の場所を定めるとき，この装置を，M系列発生器（Maximum Length Shift Register）と言う。

図−2の例は $F(x)=x^4+x+1$ になるように設計した回路と，そのレジスターの記憶状態と出力を表にしたものである。最初に与えるキーは「0000」以外なら何でもよい。




$$F(X)=X^4+X+1$$

| シフト度数 | $A_3$ | $A_2$ | $A_1$ | $A_0$ | 出力 | |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | | ⇐初期状態 |
| 1 | 0 | 1 | 0 | 1 | 0 | |
| 2 | 1 | 0 | 1 | 0 | 1 | |
| 3 | 1 | 1 | 0 | 1 | 1 | |
| 4 | 1 | 1 | 1 | 0 | 1 | |
| 5 | 1 | 1 | 1 | 1 | 1 | |
| 6 | 0 | 1 | 1 | 1 | 0 | |
| 7 | 0 | 0 | 1 | 1 | 0 | |
| 8 | 0 | 0 | 0 | 1 | 0 | |
| 9 | 1 | 0 | 0 | 0 | 1 | |
| 10 | 0 | 1 | 0 | 0 | 0 | |
| 11 | 0 | 0 | 1 | 0 | 0 | |
| 12 | 1 | 0 | 0 | 1 | 1 | |
| 13 | 1 | 1 | 0 | 0 | 1 | |
| 14 | 0 | 1 | 1 | 0 | 0 | |
| 15 | 1 | 0 | 1 | 1 | 1 | ⇐15回目のシフトで元の状態にもどる |
| 16 | 0 | 1 | 0 | 1 | 0 | |

1周期

図−2　M 系列発生器及びその状態図

$$F(X)=X^4+X+1$$

| シフト度数 | $A_3$ | $A_2$ | $A_1$ | $A_0$ | 出力 | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | | | ⇐初期状態 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | |
| 2 | 1 | 1 | 1 | 0 | 1 | 1 | |
| 3 | 0 | 1 | 1 | 1 | 0 | 1 | |
| 4 | 0 | 0 | 0 | 1 | 0 | 0 | |
| 5 | 0 | 1 | 0 | 0 | 0 | 1 | |
| 6 | 1 | 0 | 0 | 1 | 1 | 0 | |
| 7 | 0 | 1 | 1 | 0 | 0 | 1 | |
| 8 | 0 | 1 | 0 | 1 | 0 | 1 | |
| 9 | 1 | 1 | 0 | 1 | 1 | 1 | |
| 10 | 1 | 1 | 1 | 1 | 1 | 1 | |
| 11 | 0 | 0 | 1 | 1 | 0 | 0 | |
| 12 | 1 | 0 | 0 | 0 | 1 | 0 | |
| 13 | 0 | 0 | 1 | 0 | 0 | 0 | |
| 14 | 1 | 1 | 0 | 0 | 1 | 1 | |
| 15 | 1 | 0 | 1 | 1 | 1 | 0 | ⇐15回目のシフトで元の状態にもどる |
| 16 | 1 | 0 | 1 | 0 | 1 | 0 | |

図−3　M 系列発生器から 2 ビット出力の状態図

「1111」(10進法の15)から「0001」(10進法の1)まで15通りある。

又，図−3に上述と同じ列の系で2ビット出力した場合を示すが，この場合でもM系列となり15通りの出力がある。

この系列の特徴として，

① $n=2^{n-1}$ の最大周期が得られる。

② 1周期で出力させる文字の度数は，

1の数$=2^{n-1}$

0の数$=2^{n-1}-1$

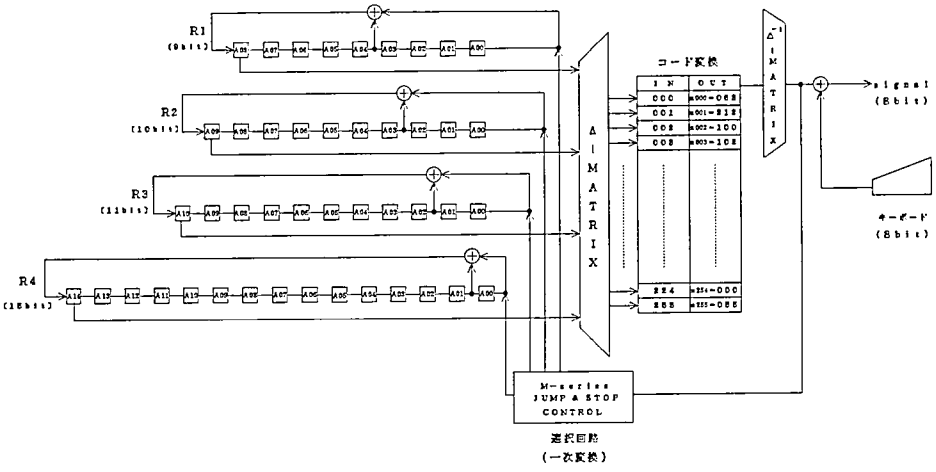
③ 連(RUN)，遷移確率は平等である。

④ 任意の字数ずらして，排他的論理和で合成した系列は，同一のM系列になる。

⑤ $n$ に対し互いに素な $k$ をとり，M系列より $k$ とびに作った新たな系列は他のM系列である。

等があげられる。

上述の事実を参考として，筆者らはM系列発生器を用い，実用性のシフトレジスター型暗号システムの作成を試みた。




図−4 システム構成図

図−4にシステムの構成を示す。上記で述べた算法により求められたM系列発生器の係数多項式を次に示す。又，本システムはビットステージの異なるシフトレジスターを4つ(R1, R2, R3, R4,)使用している。

R1 (9ビット)

$$F(x)=x^9+x^4+1$$

R2 (10ビット)

$$F(x)=x^{10}+x^3+1$$

R3 (11ビット)

$$F(x)=x^{11}+x^2+1$$

R4 (15ビット)

$$F(x)=x^{15}+x+1$$

| n | Maximum-exponent polynomial |
|---|---|
| 1 | $x+1$ |
| 2 | $x^2+x+1$ |
| 3 | $x^3+x+1$ |
| 4 | $x^4+x+1$ |
| 5 | $x^5+x^2+1$ |
| 6 | $x^6+x+1$ |
| 7 | $x^7+x+1$ |
| 8 | $x^8+x^4+x^3+x^2+1$ |
| 9 | $x^9+x^4+1$ |
| 10 | $x^{10}+x^3+1$ |
| 11 | $x^{11}+x^2+1$ |
| 12 | $x^{12}+x^6+x^4+x+1$ |
| 13 | $x^{13}+x^4+x^3+x+1$ |
| 14 | $x^{14}+x^6+x^3+x+1$ |
| 15 | $x^{15}+x+1$ |
| 16 | $x^{16}+x^5+x^3+x^2+1$ |

表－1　M系列発生器

この各シフトレジスターの係数多項式は，表－1に示すように，M系列発生器として広く知られているものを用いた。各レジスターは，ビットステージが違うため，キーのサイクルも異なりR1は$2^9-1=511$ビット，R2は$2^{10}-1=1,023$ビット，R3は$2^{11}-1=2,047$ビット，R4は$2^{15}-1=32,767$ビットになる。次に，この2進符号のビットからなる各レジスターから，下位2ビットづつを取り出して，8ビットのコードを作り出す。この様にしても前述⑤の条件を満足するため，M系列となる。この状態は，図－3に示した通りである。

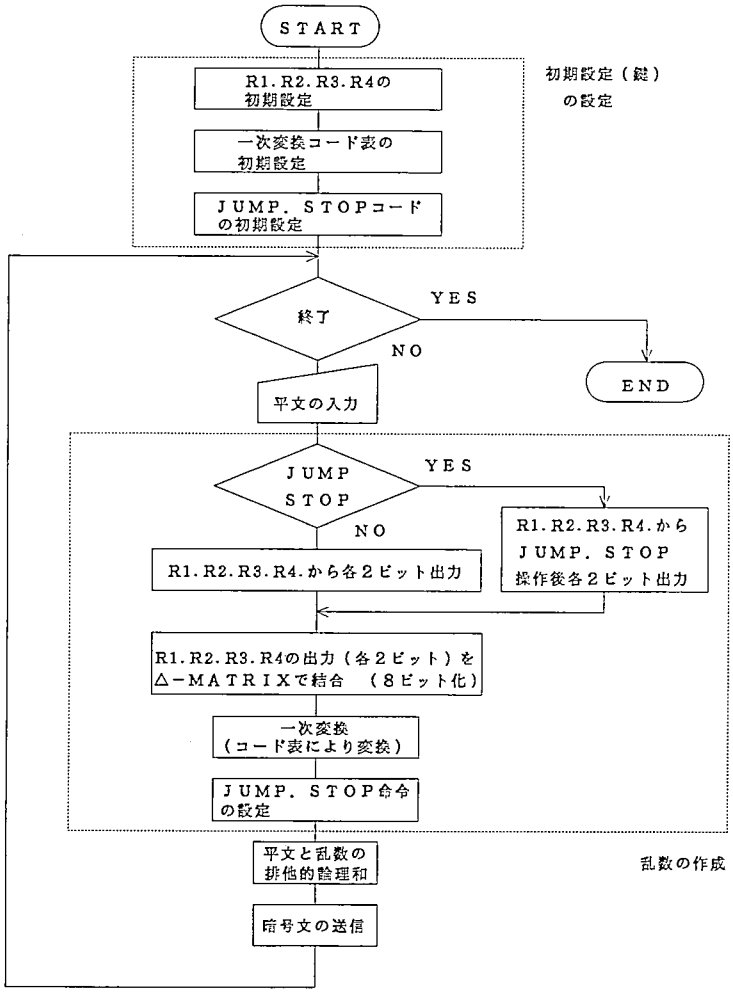
この様にして出来上がったコードに対するキーサイクルは，各レジスターの積となり，35兆0631億6033万6897ビットにもなる。

この8ビットのコードのみでも十分に擬似乱数としても利用可能であるが，実用上の暗号強度を増加させるためにコード変換を行う。これは図－4の$\Delta$－matrixにより入力の8ビットコードを256種類に展開して，乱数表によりいわゆる単一文字変換を行い，更に$\Delta^{-1}$－matrixにより，入力と異なる8ビットコードを出力する回路である。さらに暗号強度を増大させるためjump動作とstop動作を行う。jump動作とは，レジスターのシフトを2回行い，キーを1つ飛ばして（jump）出力し，レジスターのサイクルを変えるものである。この動作を各レジスターに対して独立に行う。しかし，jump動作を数多く行うとそれだけキーサイクルが減ってしまう為，stop動作を行うことを試みた。この操作は，jump動作とは逆にレジスターのシフトを0回行い（stop），同じキーを再び出力させる。jump動作と同じように，各レジスターに対して独立に行うが，jump動作の数に近似したstop動作を行えば，乱数のキーサイクルは余り変化なく暗号強度を増大させられる。この信号を制御するのが図－4中の選択回路である。

この様な方法で発生させた8ビット（0～255）の乱数をキーボードから入力した2進符号の入力データと排他的論理和（exclusive OR）の算法で合成し，入力文を暗号化する。

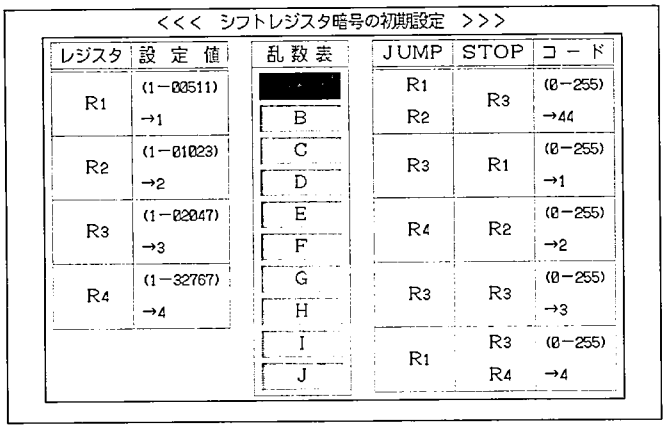
## 4. 実験

本実験は，32 ビットパーソナル・コンピュータ（NEC PC9801 DA）を 2 台使い対向通信を行った。通信方式は RS－232C 方式である。これらのソフトウェアは C 言語で書かれており，フロチャートを図－5 に示す。又，プログラムリストは本文に記載し切れぬ為省略する。



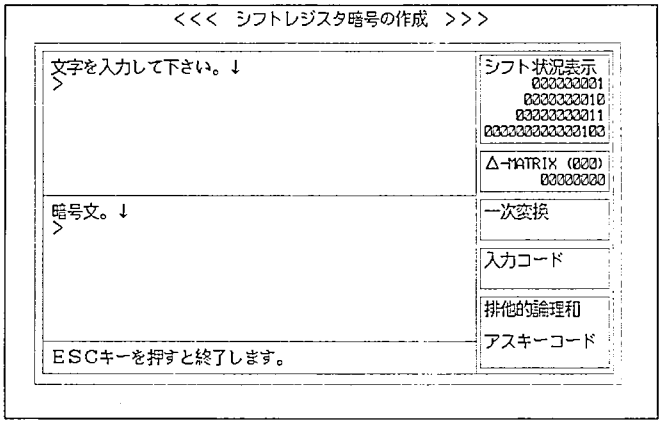

**図－5　システムのフローチャート図**

暗号化の初期設定の状況を図－6 として示す。まずキーサイクルの異なる 4 つのシフトレジスターを，それぞれ独立に 10 進数で設定する。乱数表の設定は，既に 0～255 の乱数表が A～J までの 10 表として用意されており，この中から任意の表を選んで設定する。最後に，jump と stop 動作のために，各レジスターに動作を行う度合いをほぼ等しく振り分けて置き，この動作を行う 0～255 の乱数を 10 進数で設定する。以上で暗号化の初期値（鍵）の設定を終了する。

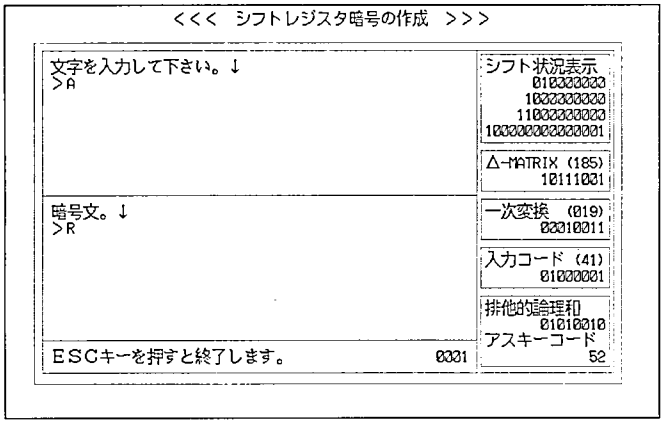



**図−6　初期設定の状況図**

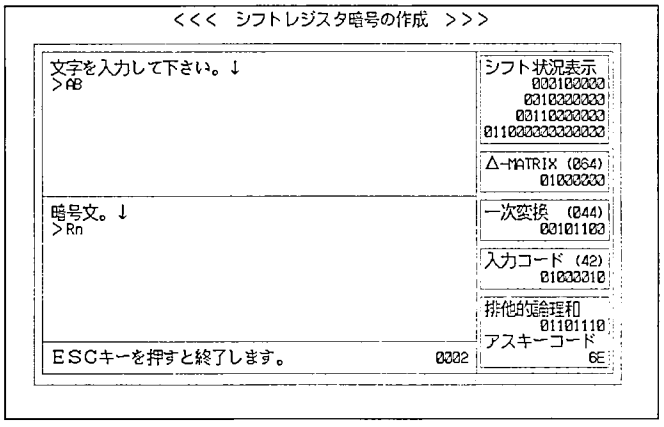
次に入力の文字が暗号化する状況を図−7から図−10に示す。図−7の「シフト状況表示」に上からR1，R2，R3，R4，の各レジスターの初期値を2進符号のビットで表示している。Δ−matrixの（　）内は同出力の10進数表示である。図−8に文字"A"を入力した状況を示す。ここでは各レジスターは2ビットづつシフトし出力している。暗号文はアスキーコードで"52"となり，「暗号文。↓」ではキャラクターコードで"R"と表示している。図−9で文字"B"を入力し暗号文を作成しているが，「一次交換」のコードが"044"を示している。これは初期設定で定義したjumpとstop動作を行うコードであり，次の入力文字に対して影響する。図−10にjumpとstop動作の行われた状況を示す。R1とR2は4ビットのシフトを行いR3はシフトしていない。これにより，入力した文字が暗号化されたことが確かめられる。



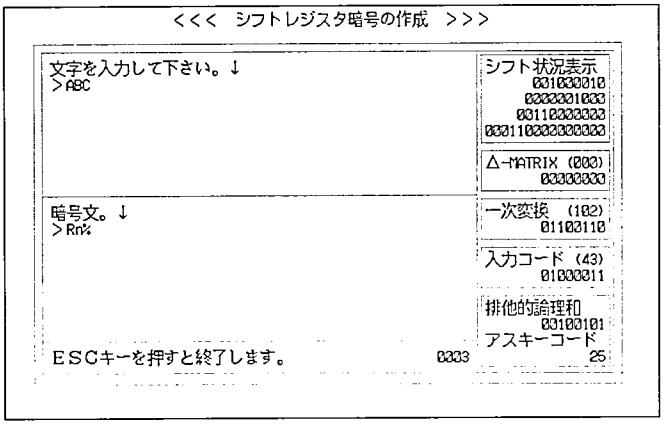

**図−7　入力文字の暗号化状況図　−その1−**




図－8　入力文字の暗号化状況図 －その 2－　文字 "A" の入力



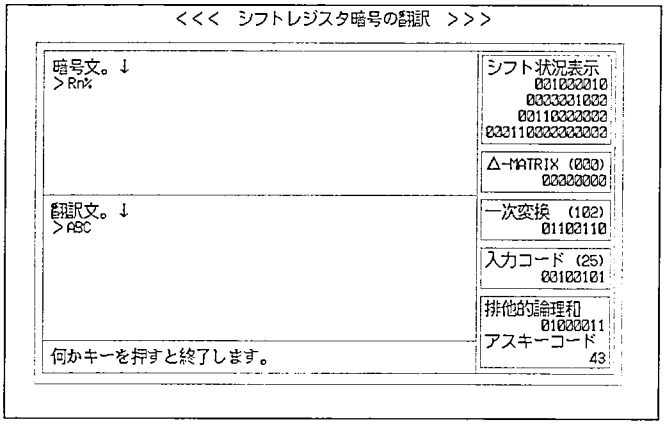

図－9　入力文字の暗号化状況図 －その 3－　文字 "B" の入力




図－10　入力文字の暗号化状況図 －その 4－　Jump・Stop 動作の状況

次に，通信で送られてきた暗号文を翻訳する方式を述べる。初期設定は，暗号化の初期設定と同じにして置く必要があり、これが翻訳の鍵になる。図－11 に翻訳の状況を示す。上段が送られてきた暗号文で，下段にそれを翻訳したものを表示している。又，右に表示した各ブロックは，暗号化の表示と同じであるが，入力コードと排他的論理和は，逆になる。これでシフトレジスター暗号を応用した暗号化と翻訳ができる。

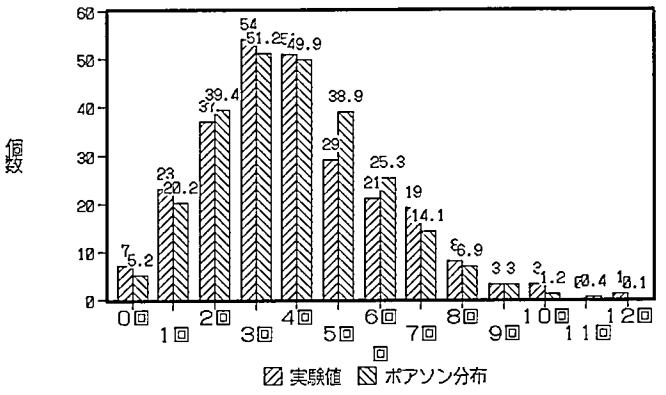
又言うまでもないが，画面の動作状態の表示等は，実際に通信を行う際には，消去する様になっている。




図－11　翻訳の状況図

## 5. 実験結果

発生する乱数についての考察を述べる。入力は，全て"A"とし本暗号機で出力した乱数を 1000 字発生させた。この乱数について種類数が 256 であることより m＝3.9 のポアソン分布に対し $\chi^2$ 検査を行った結果を図－12 に示す。




図－12　発生乱数の度数分布とポアソン分布の比較図

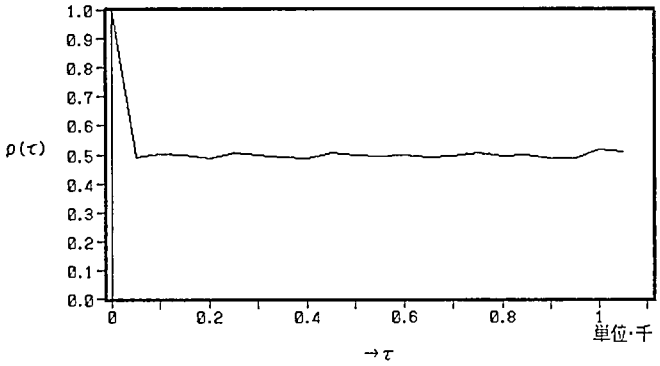
$$\chi^2_{0.05} = 16.92 > \chi^2 = 7.72$$

であるので，乱数と考えても差し支えないと言えよう。

次に同期生については，ピリオドグラム分析は原理上不可能であるので，より一般的な相関関数式

$$\rho(\tau)=\sum_{i=1}^{n}\frac{1}{n-\tau}f(x_i)f(x_i+\tau)$$

を算出して分析を行った。乱数を 1050 ビット，即ち M シリーズの 9 ビットレジスターに対し 2 周期以上計算した結果は図－13 に示した通りであり，周期性は認められなかった。




図－13　相関関数 $\rho(\tau)$

前述のクリプトラクニックや M－209 では，乱字の数 100 字もあれば周期分析が可能で乱数の解析を完了することは既に発表した[6][7][8]が，暗号強度はこの一事を以てしても，これらの機構より遙かに大きいと言える。この原因の一つは，繰り返しが確定周期の乱数源を用いず，不確定周期の乱数源を用いたことである。従って，誰にも理解し得るメカニズムで乱数を作成し得る装置として実用に供し得ると言えよう。

## 6. 実験の総括

このシステムで実験を行った結果，キーボードからの入力として，十分対向通信に対応できる処理速度である。また、暗号強度としてもパソコン通信等に対して十分である。1 度使用した乱数列は 2 度と使わないようにしても 35 兆 0631 億 6033 万 6897 文字までは，一縄用法が行えるので，何日かに 1 度の割合で初期値（鍵）の規約を改定すれば良いことになる。

システムをハードウェアに依存せずにソフトウェアのみで作成してあるため，MS－DOS の動作上では，どのコンピューターに於いても通信可能である。

## 7. 結言

本研究のシステムでは，M 系列発生器の各レジスターを固定長にしたが，これを可変長にして，初期値の設定時に任意のビット長を設定可能とすれば，暗号強度は実用上高まるものと考えられる。又，シフトレジスターの jump 数を変化させさること，及び jump や stop 動作に対するフィードバックを，入力文字と乱数を排他的論理和の算法で

合成した後で行えば，一巡周期が不確定となるので，さらに暗号強度は高まると考えられる。この様なシステムの変更に対しては，ソフトウェア依存型の暗号器であるので十分に対応可能である。結論として，本暗号器は改良の余地は在しているが，原形においてもパソコン通信は勿論のこと，具的上，暗号強度をより必要とする系に対しても簡単に即応可能であることをも含めて，実用性は十分であると考えられる。

**謝辞**

本研究に際し，ソフトウェア及び実験に協力した卒業研究生田中賢二君，宮本和也君の両氏に対して感謝します。

**参考文献**

(1) 長田　順行；"暗号"，第8章，ダイヤモンド社，1971年12月
(2) 松井　甲子；"暗号組立法入門"，第1章，森北出版，1986年
(3) 満保　雅浩，木下　宏揚，辻井　重男；"送受信者追跡の不可能な通信プロトコルに関する研究"電子情報通信学会文誌，Vol.J74－D－I，№7，pp.429－434，1991年7月
(4) 志方　　泰，"電算機情報の「盗聴」を防ぐ"，科学朝日，pp.78－82，1985年10月
(5) 土居　範久，小山　謙二；"コンピュータ・セキュリティ"，第8章，共立出版，1988年
(6) 金谷　一秀，村田　正男，志方　　泰；"時系列波の解析について"，昭和36年電気学会東京支部大会
(7) 志方　　泰，荒木　義朝；"時系列波の簡便な解析について"，昭和37年電気四学会連合大会
(8) 菅原　　茂，志方　　泰，高橋　俊朗；"予測制御における乱数波分析の一方法"，昭和38年電気四学会連合大会