【2011/ 期末】プロジェクト No.13　暗号解読の可視化　担当教員　白勢政明

RSA暗号

RSA Encryption

伊藤 拓海
Ito Takumi

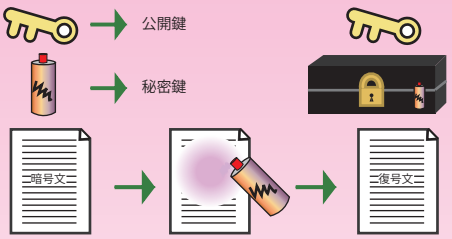
亀井 謙斗
Kamei Kento

永井 善孝
Nagai Yoshitaka

及川 真那実
Oikawa Manami

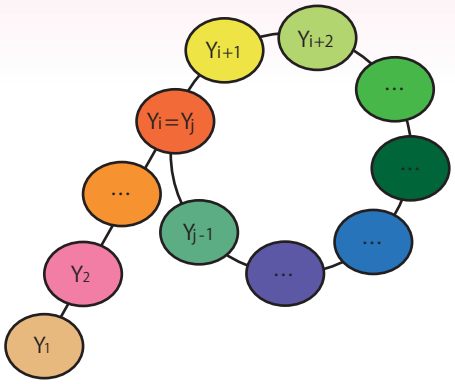
RSA暗号とは

暗号化は鍵生成、暗号化、復号の3 つのアルゴリズムで定義される。
平文　→　（暗号化）　→　暗号文　→　（復号）　→　平文
RSA 暗号は素因数分解を用いて暗号化する方法である。
大きな素数p,q を秘密鍵として決め、そのp,q を掛けたものｎを公開鍵とする。
RSA 暗号とは最も普及している公開鍵暗号方式で、公開鍵と秘密鍵を使う。
暗号の解読方法は公開されている鍵から復号の鍵を見つけることである。
つまり、RSA暗号の解読方法というのは公開鍵のｎを素因数分解することとなる。



ρ法

ρ法とはポラードにより1975年にいくつかの合成数の素因数を速く見つける方法として考えられたものである。
Ｐ法はnを合成数、dをnの未知の真約数、f(X)を既約(因数分解できない多項式を使用する。
実用上、X^2+1のようなものを使う。整数X0から始めて、次の漸化式により数列を生成する。
Xi=f(Xi-1) mod n
例としてX0=2,f(X)=X^2+1,およびn=1133とすると、数列は次のようになる。
X0=2,X1=5,X2=26,X3=677.....
また、Yi=Xi mod dとおく。d=11とするとYiの列は次のようになる。
Y0=2,Y1=5,Y2=4,Y3=6.....
Xi=f(Xi-1) mod nであるからYiはdを法としてf(Yi-1)に合同である。
dを法とする同値数は有限個しかない(すなわち、d個)から、いずれ、
あるiとjについて、Yi=Yjが成り立つ。
しかし、ひとたびこれが成り立つと以後循環し、任意の正のtについて、
Yi+t=Yj+tが成り立つ。
YiがYj に等しければ、Xi=Xj(mod d)であり、dはXi-Xjを割り切る。XiとXjが同じでない場合がほとんどであり、そうであればgcd(n,Xi-Xj)はnの真の約数である。循環の長さをcとすると、いったん尻尾を離れたら、cがj-iを割り切るような任意のiとjが使える。



成果物説明

今回実装したプログラムではアルファベット、数字、記号を使った文章の暗号化及び復号化をアスキーコード表を用いて行った。RSA暗号を実装するにあたって、２つの異なる素数p,q、その２つを掛け合わせたN、暗号化するための整数e、復号化するための整数dを用意する。eの条件としては、(p-1)*(q-1)未満であり、さらに互いに素である必要がある。
dは(p-1)*(q-1)を法としたeの逆数とする。このdは拡張されたユークリッドの互除法を使って求めることができる。またRSA暗号はNを法として暗号化が行われる。
　暗号化、復号のプログラムの流れをp=7、q=13、e=5、d=29として以下に示す。

暗号化	復号
D e c e m b e r	K x I x 5 H x *
↓ 数値化（アスキーコード表の文字、記号を扱うために数値から33を引く）	↓ 数値化し、そこから33を引く
35 68 66 68 76 65 68 81	42 87 40 87 20 39 87 9
↓ それぞれの数値をe乗する	↓ p ,q ,eの値からdの値を求め、それぞれの数値をd乗する
42 87 40 87 20 39 87 9	35 68 66 68 76 65 68 81
↓ 数値に33を足して暗号文が完成	↓ 数値に33を足して複号文が完成
K x I x 5 H x *	D e c e m b e r