RSA 暗号と Wiener's attack

1.はじめに

　RSA 暗号とは素因数分解の困難性を利用した公開鍵暗号であり、デジタル署名などにも使われている有名な暗号である。そこで今回はこの RSA 暗号がどのような仕組みで動いているのか、また数ある攻撃手法の中でも有名な Wiener's attack について調べることにする。

2.1 RSA 暗号の仕組み

　任意の素数p,qをとり、$p-1,q-1$と互いに素であるような整数eを暗号化指数として公開鍵を$\{e,N(=p*q)\}$で定める。φをオイラー関数として RSA 秘密鍵を$d\equiv e^{-1} mod\ \varphi(N)$とする。平文$M$の暗号文 C は$C=M^e mod\ N$で定義され、復号は$C^d\ mod\ N$で平文 M が得られる。このようになる理由を順に追っていく。

2.2 モジュラ逆数

　整数aと法pに対して$a^{-1}\equiv x\ mod\ p$を満たすような数xのことをモジュラ逆数と呼ぶ。これが存在するための条件はaとpが互いに素であることである。なぜなら両辺をa倍したとき$1=ax-py$であるような整数x,yを求めることは、拡張ユークリッドの互除法をすること同じであり先ほどeを$p-1,q-1$と互いに素であるようにとったのはそのためである。

2.3 オイラーのφ関数

　オイラー関数は正整数Nに対してNと互いに素である1以上N以下の整数の数を表す関数であり、$\varphi(N)$で記述される。pを素数とすると$\varphi(p)=p-1$であることは明らかなので、eを正整数としたとき、

$$\varphi(p^e)=p^{e-1}*(p-1)=p^e*(1-\frac{1}{p})$$

と書ける。つまり、Nの素因数分解が$\prod p_i^{e_i}$と表示できたならば、

$$\varphi(N)=\prod p_i^{e_i}*\left(1-\frac{1}{p_i}\right)=N*\prod(1-\frac{1}{p_i})$$

である。これを利用して、edは整数kを用いて$d\equiv e^{-1} mod\ \varphi(N)$の両辺に$e$を掛けることで

$$ed=1+k\varphi(N)=1+k(p-1)(q-1)$$

と書き表せることになる。

2.4 オイラーの定理

　nを正整数、aをnと互いに素である正整数としたときに$a^{\varphi(n)}\equiv 1\ mod\ n$が成立する。これをオイラーの定理と呼ぶ。

証明

　1 以上 n 以下で n と互いに素である整数を順に$\{x_1,x_2,\ldots,x_{\varphi(n)}\}$とする。$mod\ n$で見た時、$\{ax_1,ax_2,\ldots,ax_{\varphi(n)}\}$としたこの集合は先ほどの集合と一致する(もし一致しないと仮定すると$a(x_i-x_j)\equiv 0\ mod$ を満たす整数i,jが存在することとなり、これは矛盾である)。

つまり$x_1x_2\ldots x_{\varphi(n)}\equiv ax_1ax_2\ldots ax_{\varphi(n)}\equiv a^{\varphi(n)}x_1x_2\ldots x_{\varphi(n)}\ mod\ n$が成立する。これらを$x_1x_2\ldots x_{\varphi(n)}$で割ることで$a^{\varphi(n)}\equiv 1\ mod\ n$が得られる

復号の式は$C^d mod\ N$であったので 2.2 と合わせて次の式が得られる

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \left(\equiv M^{1+k\varphi(n)}\right) mod\, n$$

$(i)n$とMが互いに素であるとき

オイラーの定理より$M^{\varphi(n)} \equiv 1\ mod\ n$が成立するので両辺を$k$乗して$M^{k\varphi(n)} \equiv 1\ mod\ n$が成立する。よって$C^d \equiv M$である

$(ii)\ n$とMが互いに素でないとき

$M^{1+k(p-1)(q-1)} \equiv M\ mod\ N$となってほしいので、$M^{1+k(p-1)(q-1)} - M$を考えることにする。

$$M^{1+k(p-1)(q-1)} - M = M(M^{k(p-1)(q-1)} - 1)$$

MがNの倍数である時は自明なので、Mがpの倍数であり、qの倍数ではない場合を考える。このとき$M^{1+k(p-1)(q-1)} \equiv M\ mod\ p$が成立するのは明らかである。またフェルマーの小定理(オイラーの定理のnが素数である特殊バージョン)より

$M^{k(p-1)(q-1)} \equiv (M^{q-1})^{(p-1)k} \equiv 1^{(p-1)k} \equiv 1\ mod\ q$なので$M^{1+k(p-1)(q-1)} \equiv M\ mod\ N$が成立することが確かめられた。

3.1 Wiener's attack

　Wiener's attack とは RSA 暗号に対する攻撃手法の一つで、公開鍵Nに対してeが十分に小さい場合、具体的には$e < \frac{1}{3}N^{\frac{1}{4}}$の時に高速に秘密鍵$d$を復元できるというものである。

$G = GCD(p-1, q-1)$とする。

3.2 カーマイケルの定理

　$m = \varphi(n)$としたとき、nと互いに素であるようなaは$a^m \equiv 1\ mod\ n$となるが、これを満たすような最小のmを与えるのがカーマイケル関数であり、$\lambda(n)$で表す。

$n = 2^e$ならば、$e = 1$の時$\lambda(n) = 1$、$e = 2$の時$\lambda(n) = 2$、$e \geq 3$の時$\lambda(n) = 2^{e-2}$

$n = p^e$(ただしpは奇素数)ならば$\lambda(n) = p^{e-1}(p-1)$

$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$の時$LCM\{\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})\}$といったように表される。カーマイケルの定理はこのような$\lambda(n)$に対して$a^{\lambda(n)} \equiv 1\ mod\ n$が成り立つというものである。

3.3 攻撃手法

$G = GCD(p-1, q-1)$とする。

$$\lambda(n) = LCM\{\lambda(p), \lambda(q)\} = LCM\{p-1, q-1\} = \frac{(p-1)(q-1)}{G} = \frac{\varphi(n)}{G}$$

$ed \equiv 1\ mod\ \lambda(n)$より、$e$d= $K\lambda(n) + 1$を満たすような整数Kが存在する。

$$k = \frac{K}{GCD(K, G)}, g = GCD(K, G)\text{とおくと、} ed = \frac{(p-1)(q-1)k}{g} + 1$$

これを両辺dpqで割ると

$$\frac{e}{pq} = \frac{k(1-\delta)}{dg}$$

が得られ、

$$\delta = \frac{p + q + 1 - \frac{g}{k}}{pq}$$

となり、δが十分に小さい時に連分数展開をすることによって$\frac{k}{gd}$を推測することができる。

3.3　連分数展開

連分数展開とは次の形式で表される分数の一種である。

$$q_0 + \cfrac{a_1}{q_1 + \cfrac{a_2}{q2 + \cfrac{a3}{\cdots \cfrac{}{q_{m-1} + \cfrac{a_m}{q_m}}}}}$$

ここではa_iが全て 1 であるようなものについて考える。この時任意の分数から$\{q_0, q_1, q_2, \dots, q_m\}$を前から順番に求めていくことは可能であり、また$\{q_0, q_1, q_2, \dots, q_m\}$から元の分数を復元することも可能である。よって任意のタイミングで連分数展開を打ち切り、こうして得られた$\{q_0, q_1, q_2, \dots, q_i\}$から復元した分数はもとの分数の近似となる。あとは全てのq_iについて確かめていけばよい。こうして得られた

$\frac{k}{gd}$と$ed = \frac{(p-1)(q-1)k}{g} + 1$から e はわかっているので$(\mathrm{p}-1)(\mathrm{q}-1)$が復元できる。

また$N = pq$よりpqの値と$(p-1)(q-1)$の値がわかったので、これは解と係数の関係より、p, qが復元できる。

4　まとめ

RSA 暗号の仕組みと Wiener's attack について直感的ではなく理論的に理解することができた。今後別の暗号にも挑戦してみたい

参考文献

Michael J. Wiener “Cryptanalysis of short RSA secret exponents” 1987

Johannes Bl ¨omer, Alexander May “A Generalized Wiener Attack on RSA”2004

https://elliptic-shiho.hatenablog.com/entry/2015/12/18/205804