2004 年 8 月 3 日

梅暗号の概要 改定版

以下に出てくる数は全て自然数である。
r は乱数。

公開鍵・秘密鍵生成条件

$a<n, x<n, e<n$

かつ

$gcd(a, x)=1, gcd(a, n)=1, gcd(x, n)=1, gcd(e, n)=1$

かつ

$a*(x-1)+x*(a-1)<n$

($a<x$ とする)

上記の条件全てを満たす必要がある。

公開鍵

n, $e_1=e*a \pmod n$, $e_2=e*x \pmod n$

(e_1 e_2 は $e_1<n<2*e_1$ $e_2<n<2*e_2$ を満たすことが望ましい)

秘密鍵

a, x, $d(=e^{-1} \bmod n)$, d_1, d_2

($a*d_1-x*d_2=1$ を満たす自然数で最小の d_1, d_2 を拡張ユークリッドの互除法により求める)

暗号化

$C=e_1*M+e_2*r \pmod n$

$= e*(a*M+x*r) \pmod n$

暗号化できる平文 M,乱数 r の範囲は

$0<M<x$, $0<r<a$

復号

$$\begin{aligned} M' &= d*c \pmod n \\ &= d*(e_1*M+e_2*r) \pmod n \\ &= e*d*(a*M+x*r) \pmod n \\ &= a*M+x*r \ (<n) \end{aligned}$$

$M=(M'*d_1) \bmod x$

($r=a-((M'*d_2) \bmod a)$ により r を求めれるが、r は必要ない)

安全性について

$e_1=(e*a)\ mod\ n$

$e_2=(e*x)\ mod\ n$

として、 n, e_1, e_2 が与えられた時

$a*(x-1)+x*(a-1)<n$

を満たす

a, x, e を求めることが困難なことによる。

短所

・署名・認証ができない

長所

・暗号化・復号が超高速

・暗号化は、毎回 mod を行うとしても、演算回数がたった 6 回である。

・復号は、毎回 mod を行うとしても、演算回数がたった 4 回である。

・この暗号で使う数は素数である必要がない

ポイント

・メッセージの送信者は

秘密鍵 a, x, e について知らなくても

$e*(a*M+x*r)$ の計算を行えること

・M , r が互いに相手を隠しあっていること

最後に

・この pdf ファイルと一緒に配っている梅暗号の概要を知ることのできるプログラムでは
平文 M を 1024bit, 乱数 r を 64bit にしています。
既存の対称鍵暗号で 64bit 毎に暗号化しているので
r は 64bit もあれば十分と思いました。
また、M の bit 数が r に近いと平文・暗号文のふくらみ率が 2 倍近くになるので
それを抑えるために平文 M を 1024bit と大きくしています。

執筆者

梅どぶろく◆21Da3ggG3M