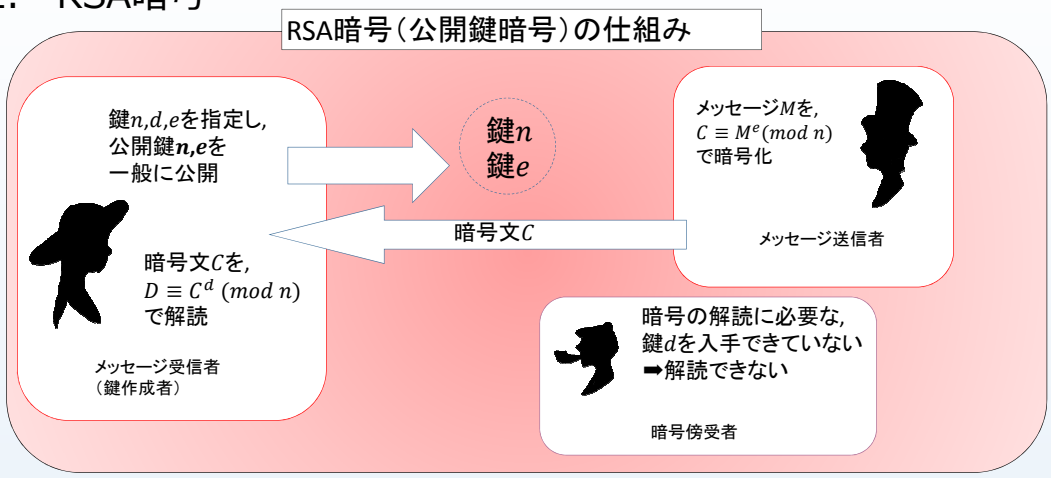
RSA暗号の安全性について

茨城県立日立第一高等学校　　根本 望史　王 宇靖

1.　動機・目的

素数の活用例としてRSA暗号があることを知り,興味を持った。RSA暗号の安全性の根拠は大きい素数の因数分解が困難なことにある。本研究では安全性について考察する事を目的とする。

2.　RSA暗号



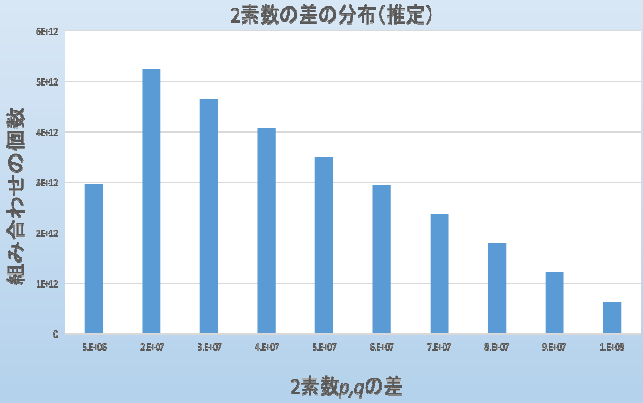
RSA暗号の定義
・暗号化…$C = M^e (mod\ n)$
・解読…$D = C^d (mod\ n)$
・$n = pq$（p,qは素数）
・dは$(p-1)(q-1)$と互いに素
・$ed = 1 (mod\ (p-1)(q-1))$

3.　プログラムによる解読

3種類のプログラムを作成し,実際に解読してみた。
①2素数の差が小さいほど早く解読できるプログラム
②2素数の差が大きいほど早く解読できるプログラム
③素数のリストを利用して解読するプログラム
使用したプロセッサ
Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz 2.50GHz

4.　素数の分布と解読効率

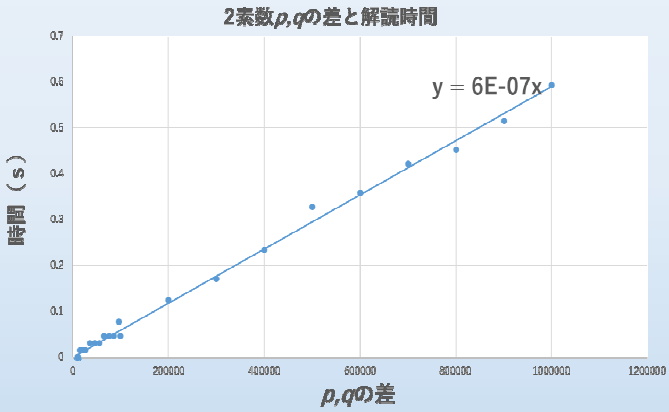
解読効率は①が最もよく、③が最も時間がかかった。
2素数の差が関係していると考えられるので、素数定理を用いて分布を調べた。



2素数の差は大きくなるにつれ、組み合わせ数は少なくなっている
→①の方法は速く解読できる場合が多くなる

5.　解読時間と安全性

暗号の安全性とは、その情報が価値を持つ間解読されないということである。
①の解読方法での解読時間を調べた。



近似曲線をもとに計算したところ、
・差が約1400億で1日
・差が約53兆で1年
解読にかかると予想される。

6.　結論

・2素数の差を利用すると効率よく解読できる。
・使う素数の桁を大きくすれば、解読されにくい暗号を作成できる。

7.　参考文献

R.L.Rivest,A.Shamir,L.Adleman
A Method Obtaining Digital Signatures and Public-Key Cryptosystems 1977-7-4