

RSA 暗号
RSA cipher
多田 洸貴 豊澤美沙 藤下実佳
Tada Kouki Toyozawa Misa Fujishita Mika

A. 研究目的

毎日学んでいる数学が普段の生活でどれくらい役に立っているのかを知りたいと思った。担当の数学科の先生に RSA 暗号は、インターネット上で広く使われている暗号で情報におけるセキュリティ確保の面において、私たちの生活になくてはならないものであるということを知ってもらい、数学的な考えが必要な RSA 暗号について調べてみることにした。また、RSA 暗号の解読方法を考えることで RSA 暗号の安全性について吟味した。

B. 研究方法

RSA 暗号は現代暗号の中でも素数を利用した暗号である。

(1) 二つの鍵

RSA 暗号には公開鍵と秘密鍵があり、公開鍵と秘密鍵は同じものではない。公開鍵は暗号するとき用いる鍵で、誰でも手に入れることができる。この鍵は2つの素数の積である。秘密鍵は復号に用いる鍵で情報の受信者のみが知っている。

(2) mod と累乗表

A と B が法 m のもと合同である時 $A \equiv B \pmod{m}$ と表す。

累乗表の数字を、mod の数以下で表しているのが mod の累乗表である。

累乗表は以下の通り。

a	a ²	a ³	a ⁴	a ⁵	a ⁶
1	1	1	1	1	1
2	4	8	16	32	64
3	9	27	81	243	729
4	16	64	256	1024	4096
5	25	125	625	3125	15625

a	a ²	a ³	a ⁴	a ⁵	a ⁶
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1

(mod 7)

(3) 実験 1

RSA 暗号の仕組みを理解するために実際に簡単な暗号を作成して解読してみた

① 作成

数字が大きくなると複雑になるので小さい数を使って考えた。

メッセージを数式化したものを 17、公開鍵を 7、33、秘密鍵を 3 とする。

元のメッセージ 17 を送

信者が公開されている 7、33 を使って暗号化する。

33 において 17 を 7 乗したら、8 と合同になり、この 8 が暗号文。

② 復号

この暗号文 8 を受信者が秘密鍵 3 を使って復号する。

法 33 において 8 を 3 乗したら 17 と合同になり、この 17 が元のメッセージと同じなので復号されたことになる。



e = 7、n = 33・・・公開鍵

d = 3・・・秘密鍵

③ 確認

mod 33 の累乗表を作ってみると、元のメッセージ 17 を 7 回かけると暗号文 8 となり、この暗号文 8 を 3 回かけると元のメッセージになっているので復号できていることがわかった。

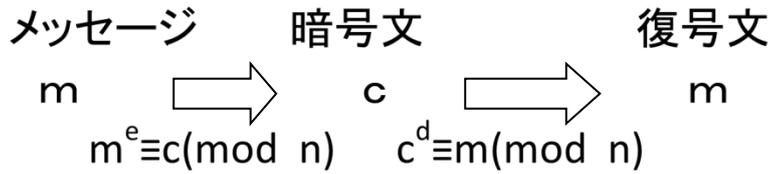
7回かける							3回かける					
a	a ²	a ³	a ⁴	a ⁵	a ⁶	a ⁷	a ⁸	a ²⁰	a ²¹
2	4	8	16	32	31	29	27	1	2
3	9	27	15	12	3	9	27	1	3
4	16	31	25	1	4	16	31	1	4
...
17	25	29	31	32	16	8	4	1	17

(mod 33)

④ 数式化

これを一般化してみる。元のメッセージを m として、公開鍵を e、n、秘密鍵を d とする。

送信者が元のメッセージ m を公開鍵 n、e を使って暗号化する。法 n において m を e 乗したらその余りは c となり、この余り c が暗号文である。この暗号文 c を受信者が秘密鍵 d を使って復号する。法 n において c を d 乗したらその余りは m になる。この余り m が元のメッセージなので復号された。



e、n・・・公開鍵
d・・・秘密鍵

C.安全性の確認

RSA 暗号が本当に安全かどうか確かめるために、第3者の立場で RSA 暗号を盗んで解読できるのか調べてみた。

さきほどの Mod 33 の累乗表を見ていたら、不規則な変化の中に全ての数が 1 になっている列があることに気付いた。

a	a ²	a ³	a ⁴	a ⁵	a ⁶	a ⁷	a ⁸	a ²⁰	a ²¹
2	4	8	16	32	31	29	27	1	2
3	9	27	15	12	3	9	27	1	3
4	16	31	25	1	4	16	31	1	4
5	25	26	31	23	16	14	4	1	5
6	3	18	9	21	27	15	24	1	6

(mod 33)

ここに注目!!!!

さらに Mod77 の累乗表を見ると a の 60 乗合同 1 となっていて、1 になるところには何か法則があるのではないかと考えた。

a	a ²	a ³	...	a ⁵⁹	a ⁶⁰	a ⁶¹	...	a ¹¹⁹	a ¹²⁰	a ¹²¹	...
1	1	1	...	1	1	1	...	1	1	1	...
2	4	8	...	39	1	2	...	39	1	2	...
3	9	27	...	26	1	3	...	26	1	3	...
4	16	64	...	58	1	4	...	58	1	4	...
5	25	48	...	31	1	5	...	31	1	5	...
6	36	62	...	13	1	6	...	13	1	6	...

(mod 77)

さらに、91 の累乗表を見ても同様に一斉に 1 になる列がありました。そこで、1 が並んでいる列の指数に注目し法則性を考えた。

a	a ²	a ³	...	a ⁷¹	a ⁷²	a ⁷³	...	a ¹⁴³	a ¹⁴⁴	a ¹⁴⁵	...
1	1	1	...	1	1	1	...	1	1	1	...
2	4	8	...	46	1	2	...	46	1	2	...
3	9	27	...	61	1	3	...	61	1	3	...
4	16	64	...	23	1	4	...	23	1	4	...
5	25	34	...	73	1	5	...	73	1	5	...
6	36	34	...	76	1	6	...	76	1	6	...

(mod 91)

はじめに言った通り公開鍵 n は二つの素数の積だから、77 は 7 と 11、91 は 7 と 13 に素因数分解ができることが分かる。これを利用すると 60 が $(7-1)(11-1)$ 、72 が $(7-1)(13-1)$ と表せることが分かった。式にしてみると $a^{60} \equiv a^{(7-1)(11-1)} \equiv 1 \pmod{77}$ 、 $a^{72} \equiv a^{(7-1)(13-1)} \equiv 1 \pmod{91}$ となっていて、それぞれフェルマーの小定理に似た形になっていた。

そこで、わたしたちは、mod を表す公開鍵 n が素因数分解できれば、フェルマーの小定理を利用して、秘密鍵なしで解読できてしまうのではないかと考え、それを数式的に示してみた。

公開鍵 $n=p \times q$ (p, q は素数) とすると
フェルマーの小定理 $x^{p-1} \equiv 1 \pmod{p}$
 $x^{q-1} \equiv 1 \pmod{q}$

これより $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

両辺に x を掛けて、

$$x^{(p-1)(q-1)+1} \equiv x \pmod{pq}$$

よって、公開鍵 n が素因数分解できれば、秘密鍵なしで解読できることが示せた。

D.RSA 暗号の安全性

しかし、簡単に解読されてしまえば、RSA 暗号が安全だとはいえない。そこで、ここでは簡単に考えた公開鍵が実際はどのくらいの桁数なのか調べてみた。

調べてみたところ、今までに素因数分解されている公開鍵 n は約 2^32 桁であり、実際に現在使われている公開鍵 n は約 6^17 桁であるということだった。

つまり、公開鍵 n はとても大きい桁数なので簡単には p と q に素因数分解することはできない。

RSA 暗号の安全性は、公開鍵 n の桁数を大きくすることで、素因数分解を難しくして確保されている。

E 謝辞

担当の木村先生、星野先生、小谷先生、中條先生、わたしたちの研究にご協力いただいたみなさまがありがとうございました。

F.参考文献

山崎圭次郎「数を考える」

三谷政昭、佐藤伸一「マンガでわかる暗号」

NHK テレビ「頭がしびれるテレビ」