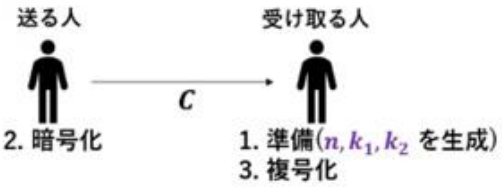
公開鍵暗号（RSA暗号）解説その2　仕組みについて　　2023.09.04

公開鍵暗号の代表であるRSA暗号については、定性的な説明は分かるものの、なぜこんな手品みたいなことができるのか。こんな簡単な方法でセキュリティは大丈夫かと疑問がわきます。そこで、公開鍵暗号の仕組みについて、補足を追加して分かり易い解説を試みました。

解説その1と同じく以下のサイトを参考にします。でもこの説明を読んだだけでは、前提などが省かれている**ためまず理解できません。**

・RSA暗号の仕組みと安全性・具体例｜高校数学の美しい物語 (manabitimes.jp)
https://manabitimes.jp/math/1146
・フェルマーの小定理の証明と例題｜高校数学の美しい物語 (manabitimes.jp)
https://manabitimes.jp/math/680

【RSA暗号の仕組み】



1. メッセージを受け取る側の準備

- 大きな素数 p, q を生成し，$n = pq$ とする
- $(p-1)(q-1)$ と互いに素な整数 k_1 を取ってくる
- $k_1 k_2 \equiv 1 \pmod{(p-1)(q-1)}$ なる k_2 を取ってくる（→補足1）
- n と k_1 を公開する（公開鍵），k_2 は公開しない（秘密鍵）

2. メッセージを送る側の暗号化方法

- 送りたいメッセージを m とする。ただし，m は n 未満の正の整数とする
- 公開鍵を用いて**m^{k_1} を n で割った余り**を計算し，これを暗号文（C とおく）とする

3. メッセージを受け取る側の復号方法

- 暗号文 C と秘密鍵 k_2 を用いて**C^{k_2} を n で割った余り**を計算すると，実はこれがもとのメッセージに一致する（→補足2）！

4. 安全性

- 暗号文 C と公開鍵 n, k_1 が分かっても（現実的な時間では）m を復元することはできない（と信じられている）

【暗号・複合がうまくいく仕組み】

- 暗号化：$m^{k_1} \bmod n$
- 復号化：$C^{k_2} \bmod n$

でうまく復号できていることを証明します。証明には**フェルマーの小定理**を使います。数学がまあまあ得意な高校生なら理解できるレベルの内容です。

高校生なら分かる？ 一寸気になる記述ですが、我慢して先に進みましょう。

証明

$m^{k_1k_2} \equiv m \pmod{n}$ を証明すればよい。

$n = pq$ なので，$m^{k_1k_2} \equiv m \pmod{p}$ を証明すれば十分（対称性より $\bmod q$ も同様）。

m が p の倍数のときは両辺ともに p の倍数よりOK。

m が p の倍数でないとき，$k_1k_2 - 1$ が $(p-1)$ の倍数となるように設定したので，整数 N を用いて $k_1k_2 = 1 + (p-1)N$ とおける。よって，

$$m^{k_1k_2} = m \cdot (m^{p-1})^N \equiv m \cdot 1^N = m$$

ただし，途中の $\equiv$ は $\bmod n$ であり，フェルマーの小定理を用いた。

【解説】

ここまでの説明文と証明を読んで**理解できるのは、この手の数学に慣れている人でもない限り、少ない**のではないでしょうか。そこであまり馴染みのない合同式をなどを、普通の四則演算に置き換えたりしながら解説を試みました。そしてもう一つ注意したいことは、この中の数式で表現される数は、整数の累乗や剰余の計算結果なので、表している具体的な数字は総て整数だと言うことです。小数とかを思い浮かべる必要はありません。

まず、 なんでいきなり**大きな素数p, qを選び、nを作れ**というのか？**⇒その理由は解説その1で書きました。**

素数の出現には規則がなく、虱つぶしに調べるしか方法がない。つまり、暗号やぶりが難しいというのが理由の一つ。二つ目は剰余計算に関して、フェルマーの小定理があり、それを使って演算すると、あっと驚く手品ができるためです。複雑な装置も、暗合表も不要で、高度な暗号化ができるのです。

平文を累乗・剰余計算して作った暗号文をさらに、同じ様に累乗・剰余計算すると、なんとその答えが元の平文に戻るという、**びっくりな仕掛けがＲＳＡ暗号です。**

つまり　　**【平文⇒累乗計算⇒剰余計算（暗号文）⇒（暗号文）累乗計算⇒剰余計算⇒元の平文】**

というわけです。

知っての通り、**剰余というのは割る数よりも、小さい数でしかも、一つ少ない種類**あります。

例えば、7の剰余は1～6まで6種類。これは割る数pが大きくなると、**1～（p-1）迄の剰余があり、剰余が平文**に戻るわけですから**、**それだけ**色々な平文の暗号化ができる**と言うことです。

この仕掛けを考えたのが、ＭＩＴの数学者リベスト、シャミア、エーデルマン。つまり頭文字をとって、**ＲＳＡ**という訳です。確か、チューリング賞をもらってます。

さて、証明に入ります。

$m^{k_1k_2} \equiv m \pmod{n}$ を証明すればよい。

確かにその通りですが、ここではこれまでの暗号化の手順を追ってこの式を**証明すればよいこと**を確認します。

暗号化・複合化の手順に沿って式を追っていくと、【mをｋ1乗し、それのnに対する剰余をＣ】として、更に【Ｃをk2乗し、それのnに対する剰余がｍと等しい】ことを証明しないといけません。これに沿うと、一般性を失うことなく【mのｋ1乗を（C+N×n）】と表し、これを【ｋ2乗】します。これは後から出てくる二項定理より【Cをk2乗した項とnを含む項】とに分かれます。この項のnに対する剰余を計算すると、ｎを含む項は消え、【Cをk2乗した項のみ】となり、【Cのk2乗のnに対する剰余と同じ】になります。

つまりこの剰余がmと同じであることを証明すれば良いことが確認できました。

$m^{k_1 k_2} \equiv m \pmod{n}$ を証明すればよい。

言い換えると、**暗号文（m^{k_1}(数字の列)の n に対する剰余）を**受信者だけが知っているk_2を使って、**累乗倍し、それの n についての剰余（＝余り）が元の平文 m（数字の列）に戻ることを証明すればよい**となります。

$n = pq$ なので，$m^{k_1 k_2} \equiv m \pmod{p}$ を証明すれば十分

これは$n=pq$であり、nの剰余はpの剰余にもなることから十分といえます。これはqについても同様です。

従って、元の式 $m^{k_1 k_2} \equiv m \pmod{n}$ も成立します。

と言うことで、ここからの証明は**n**ではなく**p**についての剰余で証明が進んでいきます。

補足1 • $k_1 k_2 \equiv 1 \pmod{(p-1)(q-1)}$ なる k_2 を取ってくる（→補足1）

補足2 m が p の倍数でないとき，$k_1 k_2 - 1$ が $(p-1)$ の倍数となるように設定したので，整数 N を用いて $k_1 k_2 = 1 + (p-1)N$ とおける。

補足1、補足2は計算が楽になるように選んだ条件で、例えば(p-1)の倍数で余りが1になる様なk2を選んでいる訳です。

いかにも簡単にk1，k2が見つかるように書いてありますが、実際にこの条件を満たすk1,k2を見つけるのは苦労します。

$$m^{k_1 k_2} = m \cdot (m^{p-1})^N \equiv m \cdot 1^N = m$$

これは$k_1\ k_2$を$1 + (p-1)N$と置き換えたので、当然の結果です。

ここで平文**m**に対し、適切に選んだk1,k2を使い、手順に従って、累乗・剰余計算をすると、平文**m**に戻ることが示されました。しかしここで疑問になるのが、$(m^{p-1})^N$ のpに対する剰余がなんで１なの？と言う事です。これを教えてくれるのが、フェルマーの小定理です。以下に説明します。

【フェルマーの小定理】

証明

任意の正の整数 a に対して $a^p \equiv a$ であることを示す （そうすれば，p と a が互いに素なとき両辺を a で割ってフェルマーの小定理がわかる）。 ←？

$a = 1$ のとき，明らかに $a^p \equiv a$

また，二項定理を用いることで，

$$(m+1)^p = m^p + 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k m^k \equiv m^p + 1$$

←多項式

よって，$m^p \equiv m$ なら，$(m+1)^p \equiv m+1$

以上から数学的帰納法より，全ての a に対して $a^p \equiv a$

この証明には数学的帰納法が使われています。

$a=1$の時はaをpで割った時の剰余なので、明らかに $1 \equiv 1 \pmod{p}$ つまり $a^p \equiv a$

$a=m$のとき、二項定理を使うと $(m+1)^p$ は上記　の多項式に展開できます。

ここで問題になるのはΣ項の係数ですが　　$_pC_k = \frac{p!}{k!\,(p-k)!}$　　となり

この係数には必ずpが乗数として含まれるので、pに対する剰余は０。従って、全体の剰余は　　$m^p + 1$。
つまり、$a = m + 1$でも、$(m+1)^p \equiv m^p + 1$　よって, $m^p \equiv m$ なら, $(m+1)^p \equiv m + 1$　　となります。
つまり、数学的帰納法によりすべてのmに対して、$m^p \equiv m$が証明されました。
ここで、両辺を**mで割ると、$m^{p-1} \equiv 1$　$(mod\ \mathrm{p})$**となり、めでたく

$$m^{k_1 k_2} = m \cdot (m^{p-1})^N \equiv m \cdot 1^N = m$$

が証明でき、暗号が復号できることになります。つまり**ＲＳＡ暗号の仕組みが正しいと証明できた**訳です。
しかし、ここで【両辺をmで割ると】となっていますが、合同式でも普通に割れるのかという疑問がわきます。
ここでは合同式の定理を使わず、普通の演算を使って証明します。
$m^p \equiv m$　　を仮定すると、一般性を失うことなく　　m^p ＝m＋N×p　（等式）
両辺をｍで割ると　　m^{p-1} ＝1+(N×p)/m　　左辺が整数なので(N×p)/ｍも整数。これはpを含むので
pで割り切れ、pに対する剰余は0となります。結局、１のみが残って m^{p-1} ≡1 (mod p）が証明されました。