RSA 暗号の仕組み

小林健太（一橋大学経営管理研究科）

RSA 暗号は，現代のインターネット上で広く使用されている公開鍵暗号として，最初に考案されたものである．RSA 暗号を理解するためには群論から理解する方が見通しが良いのだが，ここでは，予備知識なく理解できることを優先して，代数学の知識は仮定せずに解説する．

インターネットでは，情報は複数のサーバーを経由しながら伝達されていく．例えば，パソコンやタブレット等の端末でウェブページを閲覧するときには，まず，端末からプロバイダ等のサーバーにリクエストが送られ，そのリクエストが複数のサーバーを経由して目的とするウェブサーバに届き，そのウェブサーバーがリクエストに応じてウェブページの内容を返すと，その情報がまた複数のサーバーを経由して端末に送られる．メールもインターネット上の複数のサーバーを経由してやり取りされている．

インターネット上では，情報は複数のサーバーを経由して伝達されるので，途中で盗み見られたり改竄されたりする恐れがある．サーバーがクラッキングされたり，そもそもサーバーの管理者が悪意を持っている可能性もある．また，ケーブルに直接特殊な機器を取り付けることでケーブルを流れている情報を読み取ったりすることも出来る．そのため，ネットショッピング等で個人情報やクレジットカード番号等を送信する際には，暗号化が必須となる．

暗号としてすぐに思いつくのは，a → k，b → s，c → u，というように，文字を置き換える暗号である．どの文字をどの文字に置き換えるかを，あらかじめ送信者が受信者に伝えておけば，受信者は暗号を解読（復号化という）することができる．このように，暗号化と復号化の方法を送信者と受信者で共有するような方法を共通鍵暗号という．鍵という言葉は，暗号化や復号化の方法やそのためのキーワードを意味している．例えば文字を置き換える暗号の場合は，置き換えの対応表が鍵という事になる．イメージとしては，あらかじめ受信者と送信者で鍵を共有しておき，送信者は情報を箱に入れ鍵をかけて受信者に送り，受信者は鍵で箱を開けて情報を取り出す，という感じになる．

しかし共通鍵暗号には重大な欠点がある．もし悪意を持った第三者が鍵を入手してしまうと，その第三者は暗号を解読することが可能になってしまうのである．それを防止するためには，受信者と送信者の間で安全に鍵を配送しなければならない．そうなると結局，安全な通信を実現するための鍵を配送するために，安全な通信が必要になるという，ジレンマに陥ってしまう．

そこで開発されたのが公開鍵暗号である．公開鍵暗号は，上の箱と鍵の例でいうと，箱を閉める鍵と開ける鍵が異なるような暗号である．具体的には，情報の受信者は，閉める鍵を公開鍵として世間に広く公開しておく．一方で，開ける鍵は秘密鍵として大事に保管しておく．情報の送信者は，情報を箱に入れ，受信者が公開している公開鍵を使って閉めて

から受信者に送る．受信者は秘密鍵を使って箱を開ける，という流れになる．もし第三者が箱を入手しても，箱を開ける秘密鍵を入手しないかぎり箱を開けることはできない．

RSA 暗号では，公開鍵暗号を実現するために素数を用いる．まず，二つの素数 p, q を決める．ただし，積 $n = pq$ は暗号化したい数字の最大値より大きくなるものとする．例えば，暗号化する数字が 1Byte の場合は $n > 255$ となるように決める．

適当な自然数 r を取り，$r(p-1)(q-1)+1 = de$ となるような整数 d, e を求める．ただし e も d も 1 より大きくなるように取る．

n と e は受信者が公開鍵として全世界に公開する．d は秘密鍵として受信者が秘密にしておく．つまり，送信者は公開鍵 (n, e) を用いてメッセージを暗号化して受信者に送り，受信者は秘密鍵 d を用いてメッセージを復号することになる．具体的には，以下のように計算する．

平文 m を暗号化するには，m^e を n で割った余りを c とし，c を暗号文とする．

暗号文 c を復号化するには，c^d を n で割った余りを求める．そうすると m に戻る．

例として

$$p = 19,\ q = 23,\ n = 437,\ r = 2,\ e = 13,\ d = 61$$

の場合を考えてみよう．$m = 138$ を暗号化するには，$m^e = 138^{13}$ を 437 で割った余りを求めて $c = 207$ が得られる．逆に，$c = 207$ を復号化するには，$c^d = 207^{61}$ を 437 で割った余りを求めると $m = 138$ が得られ，もとの値に戻る．

通信を傍受した人がいるとして，その人が n と e から秘密鍵を割り出すには，$de - 1$ が $(p-1)(q-1)$ で割り切れるような d を求める必要がある．それには p と q が必要なので，n を素因数分解する必要がある．上の例のように，n が小さいときには素因数分解は容易だが，n が大きい場合，具体的には 10 進数で 200 桁以上になると，n を素因数分解するのは非常に困難となる．このことから，RSA 暗号の強度は素因数分解の困難さに大きく依存していることがわかる．

以下，補足しておく．

1. 今回の説明では r を決めてから e と d を求めたが，これは説明を簡単にするためにそうしたのであり，実際に使われる際には，e もしくは d のどちらかを先に決めて，それからもう一方を求めるようなアルゴリズムが用いられている．具体的には，ユークリッドの互除法を用いることで，e か d のどちらかを先に決め，次いでもう一方を効率良く求めることができる．

2. 本稿は，あくまで RSA 暗号の原理について説明したものであり，実際に公開鍵暗号として運用する上では，セキュリティーの面で考慮しなければならなことが多数ある．例えば，p と q を近い値に取ったり，d や e を小さな値に取ったりすると，それに応じた攻撃

法があり，セキュリティーが低下することが知られている．他にも，やってはいけないとされることが多くあるので，実際に使用する場合には注意すること．

3. 暗号化や復号化の際には，m^e や c^d を n で割った余りが必要になる．m^e や c^d を計算してから余りを求めると，計算の途中で非常に大きな数になってしまうので，実際には剰余系の考え方を用いて，一回掛け算するごとに n で割った余りを求める．

a, b を整数とするとき,「$a \times b$ を n で割った余り」は,「(a を n で割った余り) $\times$ (b を n で割った余り) を n で割った余り」に等しいので，常に，余りだけを考えて計算すればいいのである．

4. アルファベットを一文字ずつ暗号化するなど，暗号化の単位が小さい場合には，秘密鍵を割り出さなくとも暗号が解読されてしまうことがある．例えば，英語においてはアルファベットの中で “e”が一番多く使われるので，暗号文の統計的な情報を解析することにより，“e”を暗号化した数字がわかってしまう．また，n が小さいと，簡単に素因数分解できてしまうので，実際には n を大きく取り，何文字かまとめて暗号化する．

例えば，n を 2^{1024} =179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624224137216 より少し大きいくらいに取れば，1024bit（128Byte），すなわち半角 128 文字をまとめて暗号化することができる．

5. c^d などの累乗を計算するときには，必ずしも c を $d-1$ 回掛ける必要はない．例えば c^{61} を計算する際には

$$c^2 = c \times c,\ c^4 = (c^2) \times (c^2),\ c^8 = (c^4) \times (c^4),\ c^{16} = (c^8) \times (c^8),\ c^{32} = (c^{16}) \times (c^{16})$$

と計算しておき,

$$c^{61} = (c^{32}) \times (c^{16}) \times (c^8) \times (c^4) \times c$$

とすれば 9 回の掛け算で済む（さらに効率化する方法もある）.

以下は数学的な話である．

暗号化したものを復号化すればちゃんと元に戻るということを数学的に説明する．まず，p を素数，k を p で割れない整数としたとき，$k^{p-1}-1$ が p で割れることを示す（これはフェルマーの小定理と呼ばれる定理である）.

任意の整数 a, b について，$(a+b)^p$ を p で割った余りと $a^p + b^p$ を p で割った余りは等しい．これは，$1 \leq s \leq p-1$ に対して二項係数

$$\binom{p}{s} = \frac{p!}{s!(p-s)!}$$

が p で割り切れることからわかる（素因数として，分子は p を持ち，分母は p を持たないので）.

よって，$k > 0$ のとき，k^p を p で割った余りは $(k-1)^p + 1^p$ を p で割った余りに等しい．これを繰り返すことにより，k^p を p で割った余りと，$1^p + 1^p + \cdots + 1^p = k$ を p で割った余りが等しいことがわかる．よって，$k^p - k = k(k^{p-1} - 1)$ は p で割れる．仮定より k は p で割れないので，結局，$k^{p-1} - 1$ は p で割れることになる．剰余の性質より，これは p の倍数でない一般の整数 k について成り立つ.

さて，平文 m を暗号化して復号化すると，復号文は $(m^e)^d$ を n で割った余りになるが，それは

$$(m^e)^d = m^{ed} = m^{r(p-1)(q-1)}m$$

と書ける．ここで，フェルマーの小定理より，m が p の倍数でないとき $m^{r(p-1)(q-1)} - 1$ は p で割り切れる．よって，任意の整数 m について $(m^{r(p-1)(q-1)} - 1)m$ は p で割り切れる．同様にして $(m^{r(p-1)(q-1)} - 1)m$ は q でも割り切れる．従って n で割り切れる.

以上より，$1 \leq m \leq n-1$ のとき，$(m^e)^d = m^{r(p-1)(q-1)}m$ を n で割った余りは m となり，暗号化して復号化すると元に戻ることがわかった.