公開暗号方式

代表例

RSA 素因数分解を用いたもの

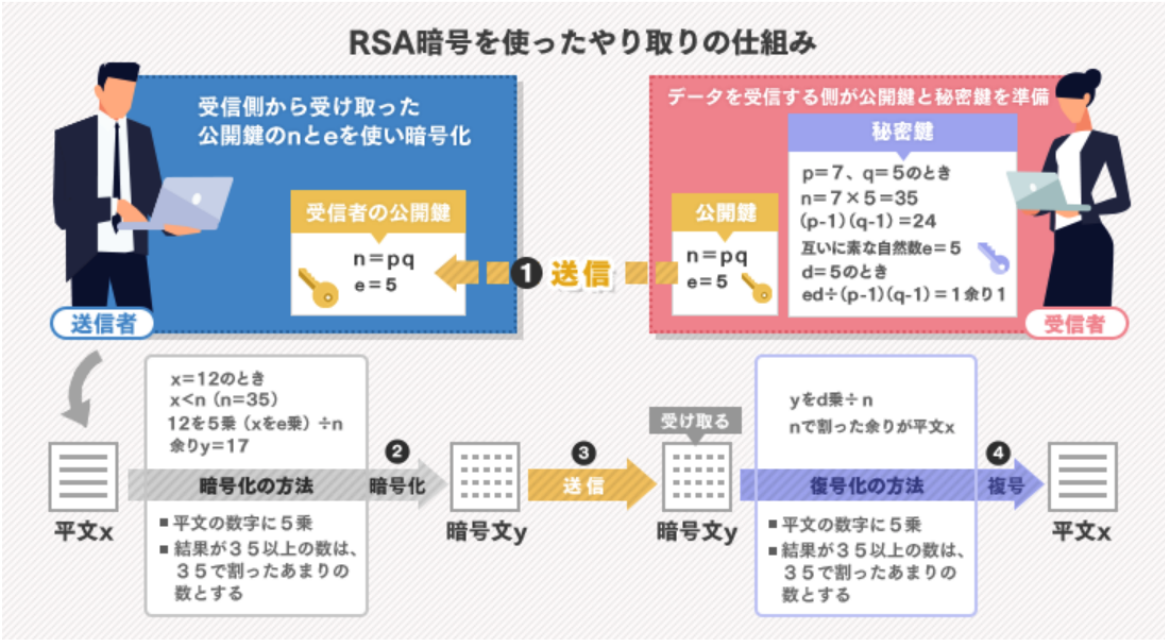
https://it-trend.jp/encryption/article/64-0056#chapter-1

公開鍵暗号方式とは、暗号鍵と復号鍵が別々の暗号方式です。データを解読するために使うのは復号鍵であって、暗号鍵ではありません。

つまり、暗号鍵は第三者に見られても問題ないということです。暗号鍵は第三者を含め誰にでも公開されて使われることから、公開鍵暗号方式と呼ばれます。

公開鍵暗号方式で使われる暗号アルゴリズムの種類はさまざまです。たとえば、DH法は鍵を交換するためのアルゴリズムです。暗号化のアルゴリズムではないため、暗号化にはほかのアルゴリズムを使う必要があります。

RSA暗号も公開鍵暗号方式で使われるアルゴリズムの一種ですが、鍵の交換だけでなく暗号化とデジタル署名を実現するアルゴリズムです。暗号とデジタル署名を両方とも達成できるアルゴリズムとして、世界で初めて登場しました。



１．受信者が公開鍵と秘密鍵を生成する

始めに、データを受信する側が公開鍵と秘密鍵を準備しなければなりません。以下の手順で鍵を生成します。

> １．異なる２つの大きな素数「p」「q」を任意にとる
> ２．n＝pqとする
> ３．（p-１）（q-１）と互いに素な自然数eを任意にとる
> ４．edを（p-１）（q-１）で割った余りが１となる自然数dを任意にとる

「互いに素」とは、最大公約数が１という意味です。こうして用意したnとeを公開鍵としてメッセージ送信側に渡します。p・q・dは秘密鍵であるため公開しません。では、上の手順の具体例を見ていきましょう。

1. １．p＝７、q＝５とする
2. ２．n＝７×５＝35
3. ３．（p-１）（q-１）＝６×４＝24なため、e＝５とする
4. ４．d＝５とする。このとき、ed÷（p-１）（q-１）＝１余り１となる

２．送信者がメッセージを暗号化する

次は、メッセージの送信側が作業します。受信側から受け取った公開鍵であるnとeを使い、以下の手順でメッセージを暗号化しましょう。

1. １．送りたいメッセージを自然数xとする。ただしx＜nとする
2. ２．xをe乗し、これをnで割った余りをyとする

こうして算出されたyが暗号文です。これを受信側に送信します。では、上の手順の具体例を見ていきましょう。

1. １．x＝12とする。これはx＜nを満たす（n＝35）
2. ２．12を５乗し、これを35で割ると余りy＝17となる

３．受信者がメッセージを復号する

最後に、受信側は送られてきた暗号文yを復号し、平文を得ます。解き方の手順は以下のとおりです。

1. １．yをd乗する
2. ２．これをnで割った余りが平文xとなる

では、上の手順の具体例を見ていきましょう。

1. １．17を５乗する
2. ２．これを35で割った余りが平文12となる

復号するにはdが必要ですが、これは受信者しか持たない秘密鍵であるため、第三者には復号されません。

第三者がdを得るにはpとqが必要ですが、これらも秘密鍵です。p×qで算出されるnは公開されていますが、nからpとqを逆算するには素因数分解をしなければなりません。ここで膨大な手間がかかるため、現実的な時間では第三者に解読されることがないとされています。

RSA暗号の応用事例

RSA暗号は公開鍵暗号方式で使われ、公開鍵で施した暗号化し、秘密鍵を持つ者のみが復号できる方法です。この仕組みは、逆の方向に使うことでデジタル署名にも応用できます。

秘密鍵を持つ側が、秘密鍵によって自身の署名を暗号化します。この署名を受け取った側が公開鍵によって署名を復号できれば、その署名が公開鍵と対になる秘密鍵で暗号化されたものだと判明するのです。

その結果、通信相手が秘密鍵を持つ正規の相手であることが証明されます。この特徴から、RSA暗号は暗号化やデジタル署名の規格として広く使われています。