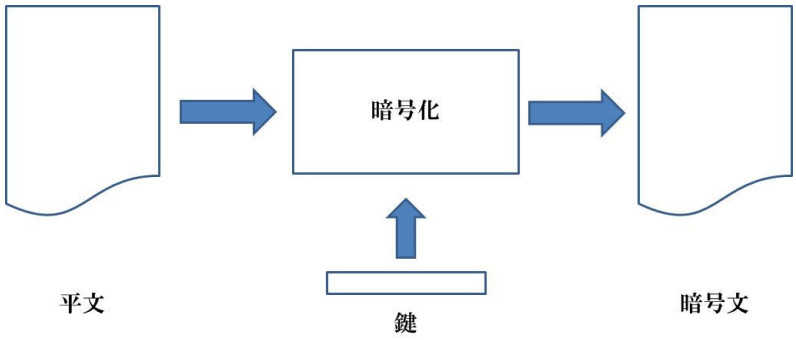
（1） 共通鍵暗号について

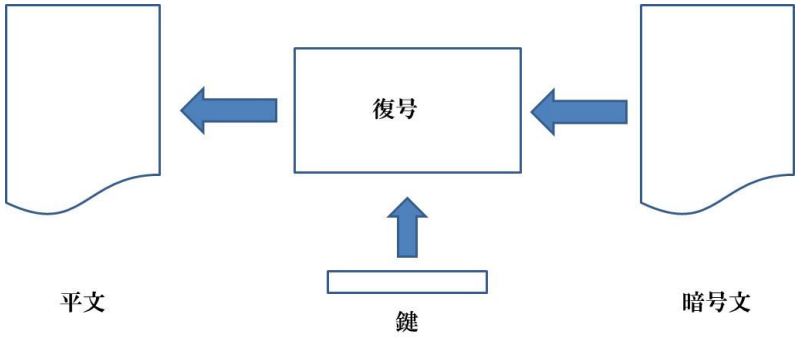
前回のご紹介の中で、共通鍵暗号については、簡単にご紹介しましたが、暗号表が鍵の役割をし、平文が「けいこをあいしてる」などと、鍵と平文をどのようにコンピュータで処理すればいいのか、具体的な動きがよくわからないのではないかと反省しました。そこで、公開鍵暗号の紹介に移る前にもう少し、共通鍵暗号についての説明をさせていただきたいと思います。

暗号の処理を図示すると下の図のようになっているというのは、前回説明しました。では、暗号化の処理というのは具体的には何をどう演算しているのかを説明してみます。どのような演算をするかということを、どのような暗号アルゴリズムを使用するか、という表現をします。アルゴリズムというのはプログラムとして、どのような手順でどのような演算をして処理をするか、というような意味で使われます。ここでは暗号アルゴリズムとして、非常に単純な演算である「排他的論理和（エクスクルーシブオア）」と呼ばれる演算を利用して暗号化を実現してみます。実際の暗号では、もっと複雑な暗号アルゴリズムを使用しています。

暗号化



復号



コンピュータの中ではデータはすべて 2 進数で処理されています。オンとオフの状態、あるいは 0 か 1 の状態の値が並んだデータです。その 1 か 0 のデータはビットと呼ばれ、

8ビットが1バイトです。よくDVDが1枚4.7GB（ギガバイト）などと言いますが、これは8ビットのデータが47億個あるというデータ量になります。コンピュータの演算としては、排他的論理和のほかに論理和（オア）、論理積（アンド）という演算もあります。それぞれ1ビットのデータ同志の演算で、下の表にそれぞれの入力と出力を示しました。論理和というのは、2ビットの入力のどちらかが、「1」であれば出力が「1」になります。論理積は2ビットとも「1」のときにだけ出力が「1」になります。排他的論理和というのは少し変わっていて、どちらかだけが「1」の時に出力が「1」になります。言い方を変えますと、入力Bが「1」の時に、入力Aの値を反転させるという言い方もできます。

論理和

入力A	入力B	出力
0	0	0
0	1	1
1	0	1
1	1	1

論理積

入力A	入力B	出力
0	0	0
0	1	0
1	0	0
1	1	1

排他的論理和

入力A	入力B	出力
0	0	0
0	1	1
1	0	1
1	1	0

さて、少し難しい抽象的な話になってしまったので、暗号の話に戻します。排他的論理和を演算として暗号化をするということは、どのようなことでしょうか。現在、実用になっている共通鍵暗号の方式では、鍵の長さは128ビットのものや256ビットのものなどがあります。かつては64ビットだったりしましたが、暗号の強度としてやや弱いため、鍵の長さの短いものは使われないようになってきました。ここの説明では鍵の長さは128ビットとしておきます。暗号化の演算は平文の先頭から、128ビットずつ取り出し、鍵の128

ビットと排他的論理和の演算をして出力を得ます。つまり、先ほどの言い方を借りますと、鍵の中の「１」のビットに対応する平文のビットが反転されて出力されてきます。これを後続のデータについても 128 ビットごとの排他的論理和の演算をした出力を並べて、暗号文として出力するわけです。

復号の際はどうなるでしょうか。暗号文の先頭から 128 ビットずつ取り出して、鍵の 128 ビットと排他的論理和をとります。先ほどは平文のうち鍵の「１」のビットに対応したビットを反転したものが暗号文となっていたわけですから、同じ「１」のビットに対応したビットを反転させればもとに戻り、平文が得られるというわけです。つまり、データの送り手と受け手が同じ 128 ビットの鍵を持ち合い、送り手が平文を暗号化して受け手に送り、受け手が復号して元の平文を得ることができるわけです。

これで、鍵が共通な暗号（共通鍵暗号）のからくりが少し理解できたでしょうか？実際の暗号はこのような単純な演算ではなくもっと複雑ですが、同じ鍵を用いて元の平文が得られるような演算になっているというところは同じです。

（２） 公開鍵暗号について

公開鍵暗号の説明に進みます。前回にも紹介しましたが、公開鍵暗号は別名「非対称鍵暗号」といいます。これは暗号化で使う鍵と復号で使う鍵が異なるため、そのように言われています。ですが、その使い道の特徴から「公開鍵暗号」と言われています。公開鍵暗号の場合は、個人、または法人や団体、Web サイトなどがその鍵の所有者となります。そして、その二つの鍵のうち一つは「秘密鍵」として所有者が他人に漏れないように保管します。もう一つの鍵は、「公開鍵」として、他者に公開します。鍵を公開するとはなんと大胆な、とお思いだと思いますが、そのことによって、いろいろな用途が生まれます。

共通鍵暗号がデータの盗聴を防ぐために使われるということは、説明しました。これはたとえ、通信路上のデータをすべて盗聴されていても、内容が解読できないので、情報の漏えいにはならないということですが、そもそも鍵そのものはどのように互いに持ち合っているのでしょうか？データを送る前に鍵を同じ通信路を使って送るのでしょうか？これでは盗聴されてしまえば、鍵そのものが盗まれてしまい、簡単に暗号文が解読され情報漏えいが防げなくなります。では郵送で別便として送りましょうか？手間がかかって仕方がありません。共通鍵暗号の場合、鍵はある程度の期間ごとに変更します。いつまでも同じ鍵を使っていてはやはり強度が保証できないとの配慮です。そんなこともあり郵送などは不便で、現実的ではありません。

そこで登場するのが公開鍵暗号です。共通鍵暗号の鍵は、乱数（規則性のないランダムな並びの数値）をその都度生成し、鍵とします。生成された鍵は、受け手の公開鍵（公開鍵暗号の公開されている鍵）で暗号化し、相手に送ります。受け手は、自分の秘密鍵（公開鍵暗号の所有者の鍵）で復号し、共通鍵暗号の鍵を得ます。公開鍵暗号はこのように情報の受け手の公開鍵で暗号化すれば、それを復号できるのは受け手だけとなるため、盗聴防止の目的にも使えるわけです。公開鍵暗号は、一方の鍵が公開されているのが前提ですから、暗号文を送る前に鍵の交換などといった手間が必要ありません。これが公開鍵暗号の威力です。さて、このようにして、共通鍵を互いに持ち合った後は、先に説明したとおり、共通鍵暗号をデータ盗聴防止に活用できるというわけです。

公開鍵暗号というのは、通常暗号化に要する時間が長いため、共通鍵暗号の鍵のような短いデータの暗号化に用い、データそのものの暗号化は共通鍵暗号を用います。

さて、公開鍵暗号の説明はまだ続きますが、つづきは次回とさせていただきます。