■#16_暗号化 共通鍵、SSL、電子署名

ここでは通信で行われる「暗号化」について解説します。

1. そもそも暗号化なんて無い方がいい

なぜ、暗号化が必要なのでしょうか。それは様々な理由によって他人のデータを見る人がいるからです。逆に、見たとしても悪用したりせず、受け流せばいいのですが、世の中そうもいかないようです。

そのために、時間とお金がどんどん無駄に捨てられてゆくことになるのです。

2. 暗号化の基本”共通鍵”

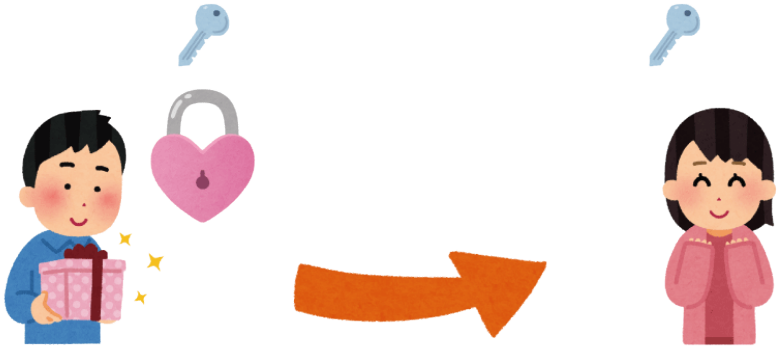
暗号化とは、特定の人だけに情報が伝えるために、関係の無い人が内容を識別できなくするものです。そのために物理的な方法として情報そのものを “隠す” ことで、情報を別のものに埋め込み、その事情が分かっている人のみ内容を取得できるという手法も暗号化の一手段です。

画像などに情報を埋め込む “ステガノグラフィー” と言う手法があります。

また情報そのものを意図的に改変し、ひと目では内容を判別することができないようにする方法があり、一般的に”暗号”と呼ばれるものはこちらになります。”暗号化アルゴリズム” は様々な種類がありその基本になる手法が “共通鍵方式“ と呼ばれるものになります。

“共通鍵方式” は暗号化と復号化に同じ鍵を用いる方式で、歴史があり非常に高速であることが特徴ですが、鍵の管理が困難であるというデメリットがあります。

ふたり同じ鍵で暗号化し複合化も行う



これで、ふたりだけでプレゼントの交換ができます。でも鍵が流出すると・・・

そのため、最近の暗号化手法では、鍵の配布に工夫をして利用しています。

3. 共通鍵を使った”暗号化”してみよう。

共通鍵を使った暗号化には様々なアルゴリズムがあるのですが、今回文字コード表を用いた暗号化にチャレンジしてみましょう。

暗号化手順

1. 配布している暗号化シートの 0-25 のセルに、アルファベットの a～z を重複しないように記入する。
2. メッセージをローマ字に置き換え、先ほどの暗号化シートの通りにアルファベットを変換する。
3. お互いに暗号化したメッセージと、暗号化シートを交換してメッセージを復号化する。

できましたか？今回メッセージを交換する対象が共通で持っている鍵が、文字コード表になります。

4. “公開鍵“の利用

先ほど、”鍵の管理が困難“ とありましたが、これを解決する手法のひとつとして “公開鍵” というものがあります。その利用には暗号化アルゴリズムの進歩により実現した。

“暗号化だけできる鍵” 、 “復号化だけできる鍵"

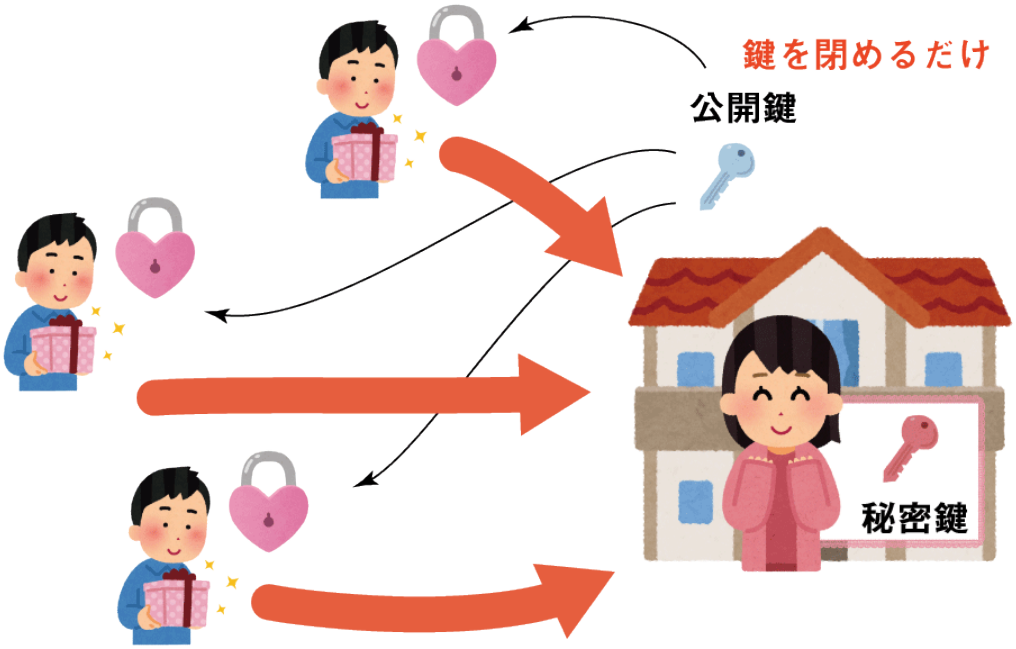
を使うことで、安全に共通鍵を交換する手法が考え出されました。
それぞれの鍵を

“暗号化だけできる鍵” → 公開鍵 ※誰でも取得できるオープンな鍵
“復号化だけできる鍵" → 秘密鍵 ※こちらは公開しない

として利用します。

【手順】

1. 送信側は、受信側が公開している「公開鍵」を取得する。そして取得した「公開鍵」で、送信するデータを暗号化して送信する
2. 受信側は、受け取ったデータを「（受信側のみ保持している）秘密鍵」で復号化して、データを取得する



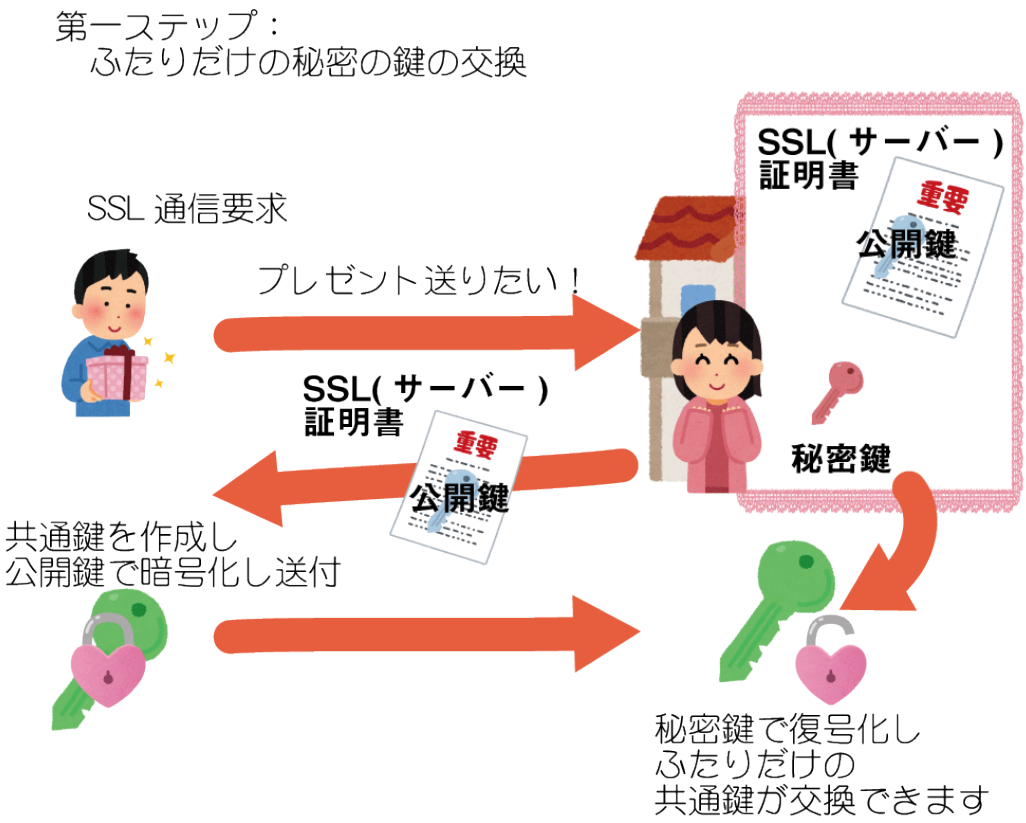
5. 2つの方法を用いて SSL

SSL は次の 2 つのステップで暗号化通信をおこないます。

【1 STEP】～通信内容を暗号化するための「共通鍵」を、クライアント/サーバー間で共有する～

1 STEP では「公開鍵暗号方式」で、通信内容を暗号化するための「共通鍵」を、クライアント/サーバー間で共有します。

1. 「クライアント」から、"SSL 通信をしたいです"と、「サーバー」へ要求する
2. 「サーバー」は、"了解"と言って、公開鍵を含めた SSL（サーバー）証明書を、「クライアント」へ送信する
3. 「クライアント」は、受け取った証明書の認証状況を確認しつつ公開鍵を取り出し、クライアント側で生成した「共通鍵」を暗号化して、「サーバー」へ送る
4. 「サーバー」は、受け取った暗号データを、秘密鍵を用いて復号化し、「共通鍵」を取得する



この流れで、最終的に「共通鍵」をクライアント/サーバー間で共有することができます。

次のステップでは、この「共通鍵」を利用して、実際の通信データ（個人情報やログイン情報）を暗号化していきす。

【２STEP】～共有した「共通鍵」で、データを暗号化して通信する～

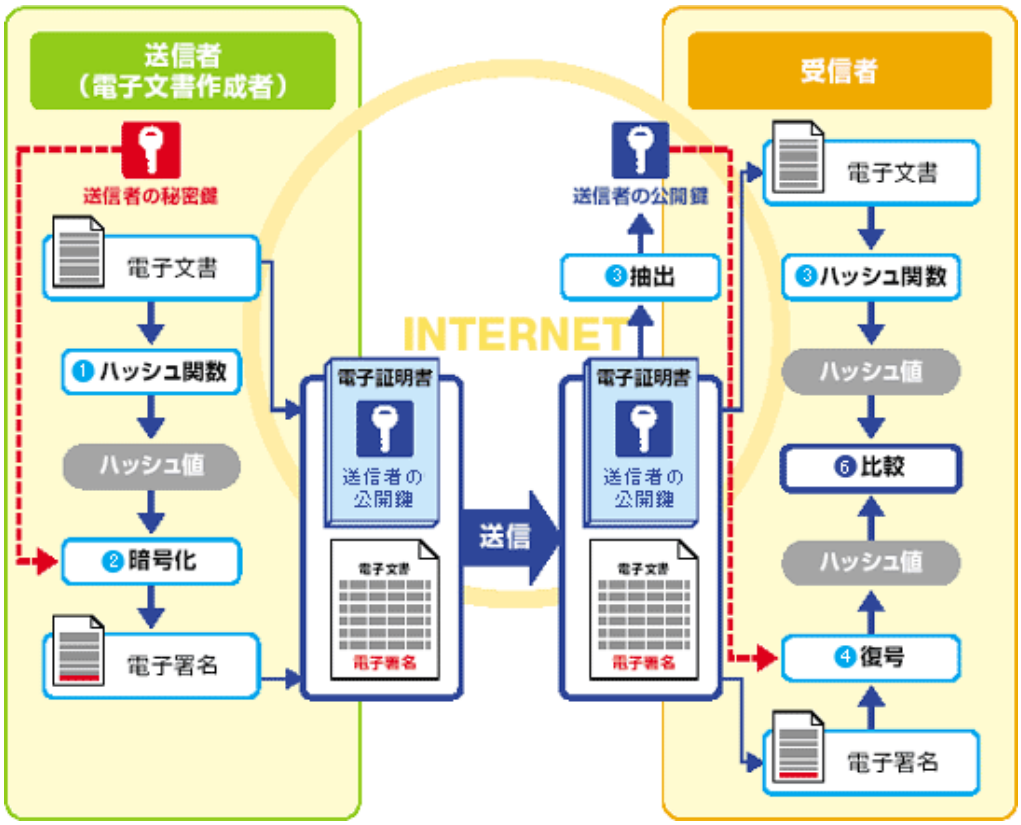
２step では、”１step で共有した共通鍵”を用いた「共通鍵暗号方式」で、実際の通信データ（個人情報やログイン情報）を暗号化して通信します。

1. 「クライアント」が、通信データを「共通鍵」で暗号化し「サーバー」へ送信する
2. 「サーバー」は、受け取った暗号データを「共通鍵」で復号化し、データを取得する

6. 公開鍵の違った使い方：電子署名

電子署名では情報そのものを暗号化するのではなく、情報そのものの妥当性を保証します。

その際に、公開鍵を下記のように利用します。



GC2018 コンピュータ概論Ⅱ

参考資料：興味ある人はこんなの見ると面白いかも

○総務省　　国民のための情報セキュリティ　暗号化の仕組み

○シマンテック　　簡単にわかる暗号の歴史

○スライドシェア　　暗号化の歴史　Takashi Abe

○チェックポイント・キーワード：

・共通鍵
・共通鍵のメリット
・SSL/TSL
・公開鍵
・SSL 証明書
・鍵の交換

図は　かわいいフリー素材いらすとや

GC2018 コンピュータ概論Ⅱ

暗号化シート

0 “A”	1 “B”	2 “C”	3 “D”	4 “E”	5 “F”	6 “G”	7 “H”	8 “I”	9 “J”

10 “K”	11 “L”	12 “M”	13 “N”	14 “O”	15 “P”	16 “Q”	17 “R”	18 “S”	19 “T”

20 “U”	21 “V”	22 “W”	23 “X”	24 “Y”	25 “Z”

暗号化メッセージ

復号化

↓
