情報の科学
１学期
第９回授業スライド

千葉県立八千代東高等学校
情報科　谷川　佳隆

セキュリティのための技術

教科書P72～P73

スライド構成

- 問
- 意味調べ
- まとめ

問

問

- コンピュータではセキュリティのための技術にどんなものがあるか？

意味調べ

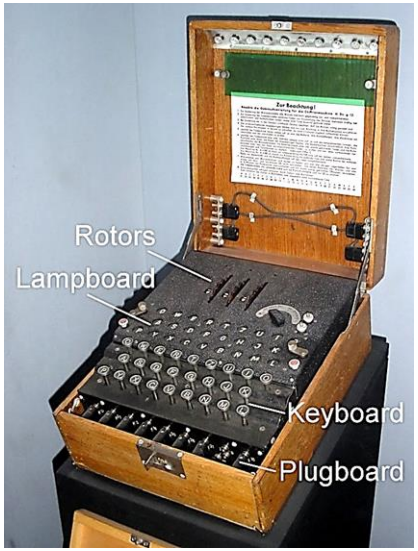
次の言葉の意味は

暗号	

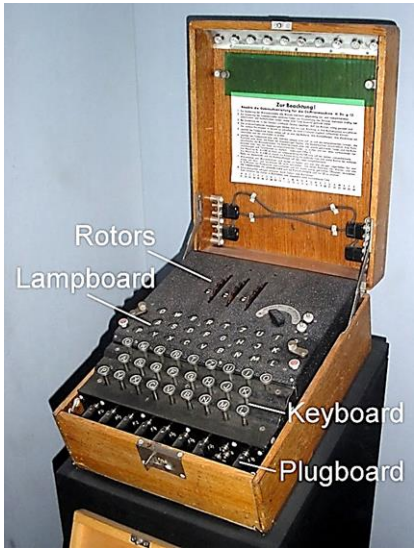
意味

暗号	第三者に通信内容を知られないように行う特殊な通信（秘匿通信）方法のうち、通信文を見ても特別な知識なしでは読めないように変換する表記法（変換アルゴリズム）のこと

次の画像は何



エニグマ



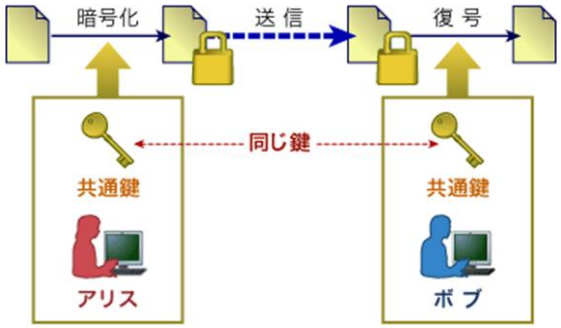
エニグマ (Enigma) とは、第二次世界大戦でナチス・ドイツが用いたローター式暗号機である。

まとめ

暗号

データの盗聴などの不正行為に対応するために、
第3者が見ても意味が分からないようにすることを（暗号化　）という。暗号化する前のデータを（平文　）といい、暗号化されたデータを暗号文という。また、暗号文を平文に戻すことを（復号　）という。暗号化や復号する際に必要な規則（手順）を（カギ　）という。

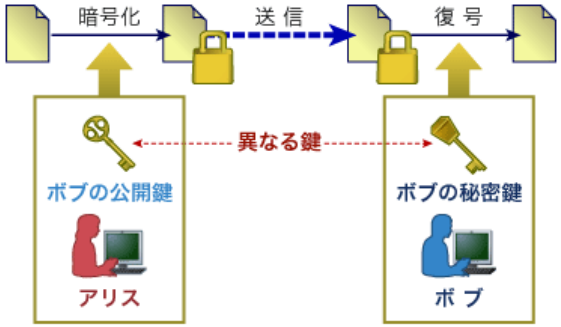
共通鍵暗号方式



データの暗号化を同じ1つの鍵で行う方式を（共通鍵暗号方式）という。この方式で有名なのが（シーザー暗号）である。同じ鍵で済むので処理速度が（早く　）なるが、鍵をどう秘匿に渡すのかが弱点がある。

画像引用
https://www.itmedia.co.jp/enterprise/articles/0504/26/news003.html

公開鍵暗号方式

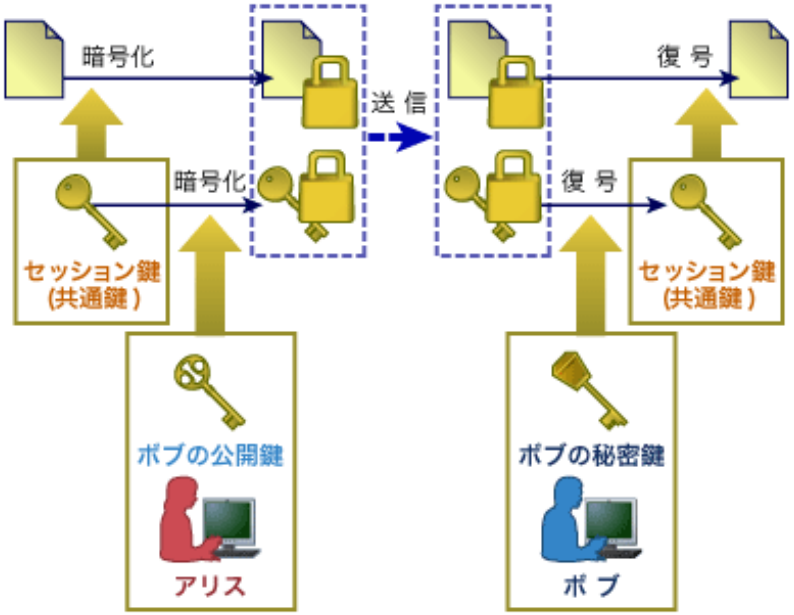


対になっている異なる2つの鍵を利用する方式を（公開鍵暗号方式）という。どちらかの鍵で（暗号化　）し、もう片方の鍵で（復号　）する。1つの鍵からもう片方の鍵は作り出すことはできない。2つの鍵が必要なため、1つをなくしても復号されず安全であるが、処理速度が（遅く　）なるという欠点がある。（受信者　）は、1つの鍵（公開鍵　）を暗号化用として公開し、もう一方の鍵（秘密鍵　）を復号するため秘密にしを持てばよい。

画像引用
https://www.itmedia.co.jp/enterprise/articles/0504/26/news003.html

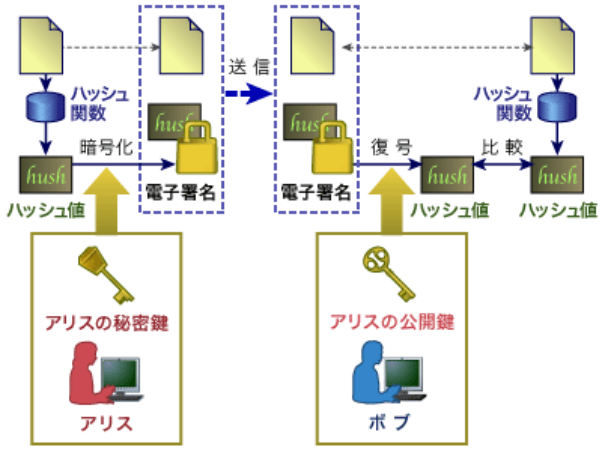
ハイブリッド暗号方式

Webページで用いられている（SSL　）では、（共通鍵暗号方式　）を使って（平文　）を暗号化・復号を行い、平文に比べて小さい共通鍵そのものを（公開鍵暗号方式　）で、暗号化・復号を行う
（ハイブリッド暗号方式　）を利用している。



画像引用
https://www.itmedia.co.jp/enterprise/articles/0504/26/news003.html

ディジタル署名



（電子署名　）は、平文の作者の本人確認とともに、データが途中で（改ざん　）されていないことを保証する（電子データ　）である。電子署名は、平文からプログラムを利用して作った（要約文　（ダイジェスト　））を（送信者　）の秘密鍵で暗号化したものである。これを平文に付加して受信者に送る。受信者は送信者から送られてきた（公開鍵　）を使った（電子署名　）を復号して（要約文　）に戻す。復号が成功すれば送信者本人から送られてきたものであることが確認できる。また、平文からプログラムを利用して（要約文　）を作り、復号した（要約文　）と比較して一致すれば（改ざん　）されていないことがわかる。電子署名は（公開鍵暗号方式　）を逆に利用している。

画像引用
https://www.itmedia.co.jp/enterprise/articles/0504/26/news003.html

参考サイト

- Enigma Machine Emulator https://www.101computing.net/enigma-machine-emulator/
- 知ってるつもり？「セキュリティの常識」を再確認：11回　暗号技術の常識(1/5) https://www.itmedia.co.jp/enterprise/articles/0504/26/news003.html