秘匿と認証

2006年度司書教諭講習
第2回
2006年 8月11日(金) 2時限目

thema

秘匿と認証

contents

1. 秘匿
   1. 暗号
   2. ステガノグラフィー
      1. (steganography：電子あぶり出し)
   3. 電子透かし
2. 認証
   1. 電子署名

秘匿と認証

1. 秘匿
   - 秘密にしておくこと [新村出編「広辞苑　第五版」岩波書店, 1998. p2254]
   - 同義語：守秘
2. 認証
   - 一定の行為または文書が正当な手続･方式でなされたことを公の機関が証明すること [新村出編「広辞苑　第五版」岩波書店, 1998. p2050]
   - 関連語：デジタル署名, 電子署名, 電子認証

秘匿の技術

1. 暗号
2. Steganography（電子あぶり出し）
3. Watermark（電子透かし）

暗号

1. 定義
   1. 暗号とは, 秘密通信のため当事者間のみが第三者に理解できないように変換した情報である. [北川高嗣 (ほか) 編「情報学事典」弘文堂, 2002. p30]
   2. 暗号とは, メッセージの外見を変えることにより, 正当な受信者にしか読めないようにする方法である[サイモン･シン著「暗号解読」新潮社, 2002.p10]

暗号の種類

1. シーザー暗号
   1. アルファベットをある文字数だけずらすというもの
2. 単文字換字暗号
   1. 文字の別の文字に置き換える方法
   2. ポー「黄金虫」, コナン・ドイル「踊る人形」
3. 多表式暗号
   1. 複数の鍵を使用する方法

シーザー暗号

単文字換字暗号

多表式暗号

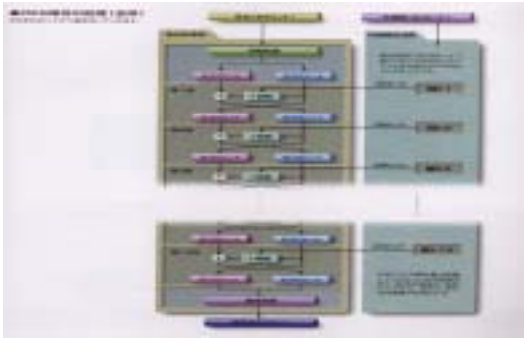
暗号と鍵

1. 共通鍵暗号
   1. 暗号の送信者と受信者が同じ鍵を使用する
   2. シーザー暗号, 単文字換字暗号など
2. 公開鍵暗号
   1. 公開鍵と秘密鍵の2種類の鍵を使用
   2. 公開鍵は暗号化専用, 秘密鍵は復号化専用

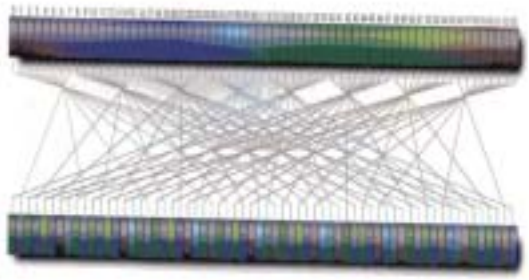
共通鍵暗号

1. DES(Data Encryption Standard)暗号
   - 実用化されている共通鍵暗号システム
   - IBMが開発
   - “データ暗号規格DES”として1977年に米国商務省が公布
   - 処理方法
     1. 平文からデータを64ビットずつ読み込む(8ビットはパリティデータ)
     2. それを64ビットの暗号にして出力

DES暗号の処理



DES暗号の初期転置の処理



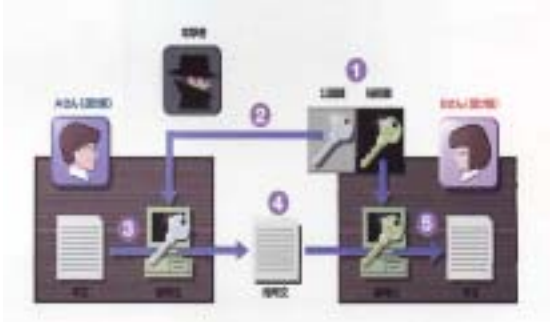
公開鍵暗号

1. 公開鍵暗号は1976年に
2. W.Diffie とM.E.Hellman らによって最初に提唱されました
3. (W.Diffie and M.E.Hellman: ``New direction in cryptography‘’Trans. IEEE on Information Theory, IT-22, No.6, 644-654(Nov. 1976)。
→DH法

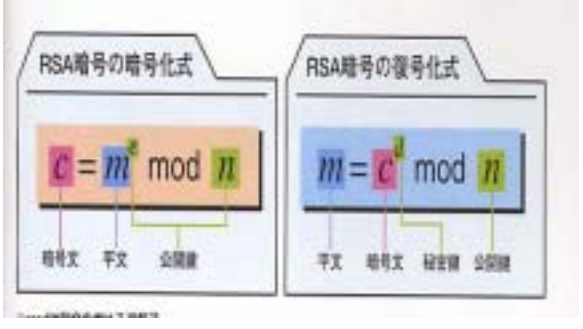
公開鍵暗号

2. DHの論文発表後、公開鍵暗号のアイデアを最もうまく実現させて見せたのが1977年のR.Rivest、A.Shamir 及び L.Adelmanらが発表した、有名な RSA暗号。(R.L.Rivest, A.Shamir and L.Adleman: ``A method of obtaining digitaland public key cryptosystems", Comm.ACM, 21, No.2, 120-126(Feb. 1978)

公開鍵暗号の原理



公開鍵暗号の鍵



鍵の生成方法

暗号

1. 暗号は人に理解できる（読める）情報を、特別な解読鍵なしには理解できない（読めない）形に“あからさまに”変形したもの
2. 秘密は保たれるが、「秘密データの存在」を隠すことは出来ない
3. 逆に秘密情報に関する関心をかき立ててしまうことになる
4. 秘密にすることで人と人との関係に悪影響を及ぼすこともある

Steganography

「秘密が存在する事実」を
他人に気付かせない技術

コンピュータデータ

1.電子あぶり出し技術
2.情報非可視化技術
3.深層暗号化技術
4.電子迷彩技術

目的

他人に見られたくない秘密情報を何か別のデータ（“封筒”、すなわち、ダミーデータ）の中に埋め込み、一見、その秘密の存在そのものを見えなくしてしまう 技術

データの取り出し

埋め込んだ秘密を取り出すには、特別な鍵を使用

Steganography

1. 見えるデータ(ダミー画像)にはあまり価値がなく、隠されているデータ(秘密情報)に価値がある
2. 秘密の隠し場所はできるだけ大きいことが必要とされる
3. たまたま秘密情報が送信中に第3者によって消されてもあまり大きな損失にはならない

Watermark

表のデータ(画像データ等)に価値がある少量で除去しにくい秘密データを埋め込む技術

画像のどこに情報を埋め込むか

1. ビットプレーンの最下位ビットを画一的に秘密情報と入れ替えるもの
2. 画像の周波数分解において、ある特定の成分を置き換えるもの
3. 画像のサンプリング誤差に秘密データを埋め込むもの

電子透かし

1. 定義
   - 画像や音声などのマルチメディア・データになんらかの情報(著作者情報・サイン・ロゴマークなど)を埋め込み、隠しもたせる技術
2. 種類
   - 埋め込んだ情報が見える電子透かし(visible digital watermark)
   - 埋め込んだ情報が見えない電子透かし(invisible digital watermark)

透かし_紙

透かし_紙

電子透かし

visible digital watermark

invisible digital watermark

invisible digital watermark の特徴

1. 著作物に著作権を示す透かし情報が残りつづけること
   - 無理矢理透かし情報を取り去ろうとすると情報が劣化する
   - データ圧縮，フィルタ処理をしても透かし情報が無くならない
   - フォーマット変換しても透かし情報を取り出せる
2. 著作物のどこに透かし情報が埋め込まれているのかわかりにくいこと
   - 万遍なく透かし情報を埋め込むことができる
   - 人間の感覚では知覚できない
3. 透かし情報を埋め込んでも著作物はオリジナルの状態をとどめられること
   - 冗長部分に雑音として埋め込むため，人間が知覚できない

電子透かしの利用方法

1. 著作権情報の記録
2. 違法コピー者情報の追跡
3. IPアドレスの履歴記録
4. 違法コピーの防止
5. 改ざん防止

認証

1. 認証とは
   - 自分が自分であることを第三者に証明すること
2. 方法
   - デジタル署名
3. 利用技術
   - RSA暗号
4. 利用方法
   - デジタル署名とは，暗号化された署名情報を電子メッセージに付加する技術
   - 電子メッセージの作成者や発信者を識別し，署名後のメッセージが改ざんされていないことを証明する
   - 電子メッセージの本体は暗号化されないので，メッセージの内容を隠す目的で利用することはできない。