情報Ⅰ

2-1-16　　通信の暗号化
2-1-17　　ディジタル署名
2-1-18　　ディジタル証明書

2-1-16　通信の暗号化

(1)　最古の換字式暗号：シーザー暗号(文字から文字に1文字単位で変換)

3文字前シフトの場合　　暗号：EC➡BZ　　復号：BZ➡EC

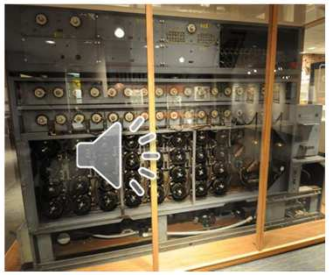
x	y	z	a	b	c	d	e	f	g
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
u	v	w	x	y	z	a	b	c	d

元データ:平文

暗号化、逆を復号化

暗合文

エニグマ（Enigma)第二次世界大戦でドイツが用いたローター式暗号機
https://ja.wikipedia.org/wiki/%E3%82%A8%E3%83%8B%E3%82%B0%E3%83%9E_(%E6%9A%97%E5%8F%B7%E6%A9%9F)より画像引用



アラン・チューリング(英)第二次世界大戦にエニグマ解読のアルゴリズム開発→計算機に実装…連合軍が活用したbombe
https://japan.cnet.com/article/35115908/3/より画像引用

(2)　共通鍵

データ送信者
暗号化
例　シーザー暗合　+1
平　文　12
↓
暗号文　13

共通鍵　1

通信上の
留意点

データ受信者
復号化
例　シーザー暗合　-1
暗号文　13
↓
平　文　12

共通鍵　1

計算機を用意


た
天気
電卓
問い合わせ
電卓
電卓
関数電卓
グラフ計算
プログラマー
日付の計算
コンバーター
通貨
ボリューム
長さ
設定
0
exp
mod
n!
9
6
3
.
=
関数電卓
Modulo：a mod b
a÷b の余り
x ^ y ➡ x^y
MR
M+
M−
MS
関数
π
e
C
x²
1/x
|x|
exp
mod
(
)
n!
7
8
9
4
5
6
log
1
2
3
ln
+/−
0
スタートボタン
calc
13°C くもり
あ
8:33
2023/03/21

(3)　RSA Security　１．受信者が公開鍵と秘密鍵準備

１．受信者が２つの素数 p、q を設定
２．公開鍵 n＝pq とし、送信者に渡す
３．(p−1)(q−1)と互いに素な自然数 e 公開鍵を設定し、送信者に渡す
４．ed/(p−1)(q−1) の剰余が 1 となる自然数 d 秘密鍵を任意設定

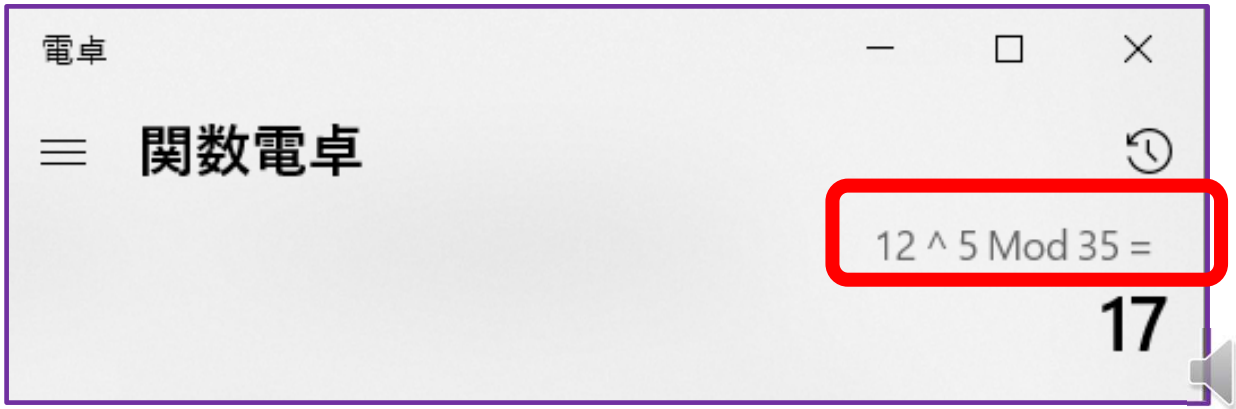
（最大公約数１）

１．p＝7、q＝5とする
２．公開鍵 n＝7×5＝35
３．(p−1)(q−1)＝6×4＝24 ➡　公開鍵 e＝5とする
４．秘密鍵 d＝5 とすると、ed÷(p−1)(q−1)＝1...1

(3)　RSA Security ２．送信者がメッセージを暗号化

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．x を e乗し、これを n で割った余りを y(暗号化) として送信

１．x = 12 とする。･･･ x<n (=35) を満たす
２．x = 12 を(e=5)乗(公開鍵)し、n=35で割る(公開鍵)
　　$12^5/35 = 7109 \cdots 17$　　余り y＝17･･･暗号文➡送信



(3)　RSA Security　３．受信者がメッセージを復号

１．暗号文 y を d乗(秘密鍵)する
２．これを(公開鍵) n で割った余りが平文 x

１．暗号文17 を 5乗　復号時に d=5 が受信者しか持たない秘密鍵
２．これを(公開鍵n) 35 で割った余りが平文 12 となる

第三者が d を得るには pとq が必要➡秘密鍵
n=pq は公開されるが、n➡p、qを逆算する素因数分解に手間がかかるため、
現実的な時間では第三者に解読されることがない

(3)　公開鍵・秘密鍵　ＲＳＡ暗号

データ送信者
公開鍵　n＝35受領
公開鍵　e＝5受領

平文12を公開鍵で暗号化
$12^5/35$の剰余17
暗号文17を送信

通信上の
留意点

データ受信者
公開鍵　n＝35作成・送付
公開鍵　e＝5設定・送付
秘密鍵　d＝5　作成

暗号文17を受信
暗号文17を復号
$17^5/35$の剰余12
平文12を確認

2-1-17　ディジタル署名

公開鍵暗号方式

公開鍵で暗号化した暗号文 ➡ 公開鍵とペアの秘密鍵で復号

秘密鍵で暗号化した暗号文 ➡ 公開鍵で復号

データ送信者Ｂ
平文をＢの秘密鍵で暗号化
暗号文（ディジタル署名）を送信

データ受信者Ａ
暗号文を受信
暗号文をＢの公開鍵で復号
平文を確認

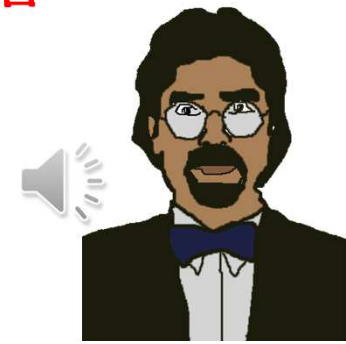
Ｂ が Ａ に文書を送信時、Ｂ の秘密鍵で暗号化

受信者 Ａ が、Ｂ の公開鍵で復号

平文に戻る・・・ Ｂ が作成した文書

＝ Ｂ の秘密鍵で暗号化された文書

この方法を署名に利用　ディジタル署名



2-1-18　ディジタル証明書

データ送信者Ｘ（Ｂのなりすまし）
公開鍵公開

データ受信者Ａ
Ｘ（Ｂのなりすまし）の公開鍵を
Ｂのものと認識

Ｂ が Ａ と通信する前、第三者 Ｘ が Ｂ になりすまして秘密鍵を作成、公開鍵を公開

インターネット上では
それが Ｂ のものとして通用してしまう

Ｘ は Ｂ になりすまして契約可能

データ送信者Å
暗合文送信

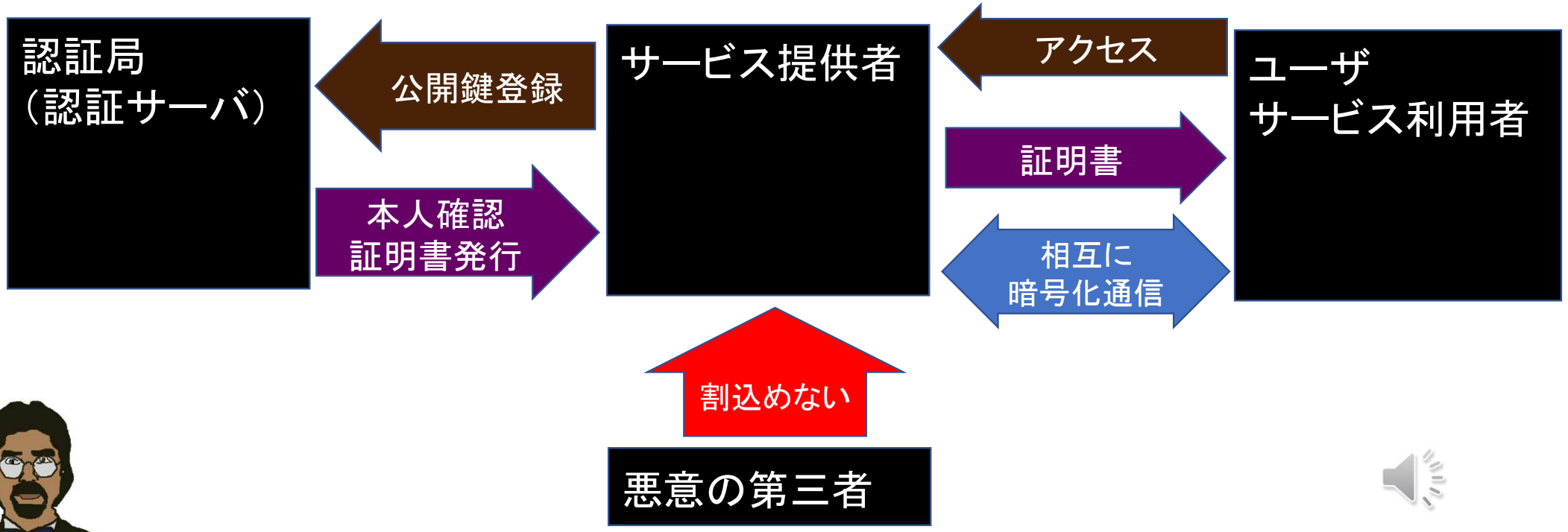
データ受信者Ｂ
平文に復号できない

データ送信者Ｘ（Ｂのなりすまし）
平文に復号できる

2-1-18　ディジタル証明書

公開鍵（ディジタル署名）が本人のものであることを、 認証局（認証サーバ） とよばれる信用できる第三者が証明するしくみ

ディジタル署名利用者は認証局に登録して、　ディジタル証明書　の発行を受ける



電子署名、電子証明書：個人・法人確認

認証局
送信者に証明書発行
証明書の正当性確認
受信者に認証局公開鍵発行

データ送信者
公開鍵の電子証明書申請
証明書受領
データ
ハッシュ値（秘密鍵で暗号化）
電子署名
公開鍵＋証明書（暗号化）

データ受信者
認証局公開鍵受領
データ
電子署名
公開鍵＋証明書（暗号）
認証局公開鍵で証明書復号

SSL　Secure Socket Layer （https://）

認証局

電子証明書発行

ユーザ側ブラウザ

SSL通信要求

証明書の正当性確認
ウェブサーバ公開鍵で証明書復号
乱数➡共通鍵作成し
サーバの公開鍵で暗号化送信
共通鍵受信（共通鍵交換）
データ（相互に暗号化）

ウェブサーバ側
公開鍵を認証局へ届け出
電子証明書

公開鍵付き証明書送信
（電子署名有り）
秘密鍵作成

乱数を秘密鍵で復号
共通鍵作成送信
データ（相互に暗号化）