 帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

**情報セキュリティ論(3)
暗号(2):公開鍵暗号**


中野秀男
帝塚山学院大学非常勤講師
大阪市立大学名誉教授、堺市情報セキュリティアドバイザー


1 情報セキュリティ論 暗号(2) 2020/5/22

1

今日の話

- ▶ 暗号の復習(3回目の暗号の基礎などをもう一度視聴)
- ▶ 公開鍵暗号
- ▶ 電子署名の仕組み
- ▶ RSA暗号



▶ 2 情報セキュリティ論 暗号(2) 2020/5/22  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2

暗号の種類

- ▶ 慣用(共通鍵)暗号
 - ▶ 暗号化鍵も復号化鍵も秘密(秘密鍵)
 - ▶ 1980年前までは、暗号はこれだけ
- ▶ 公開鍵暗号
 - ▶ 暗号化または復号化鍵を公開する暗号
 - ▶ もう1つの鍵は秘密
 - ▶ 暗号化鍵を公開: 秘匿
 - ▶ 復号化鍵を公開: 電子署名
 - ▶ ちょっと過去を
 - ▶ 1970年代に計算量の研究が盛んに
 - ▶ 解ける問題と解けない問題
 - ▶ $P \neq NP$
 - ▶ この研究の流れからRSA暗号ができた

▶ 3

情報セキュリティ論 暗号(2) 2020/5/22



3

公開鍵暗号

- ▶ 暗号解読の難易度を数学的に示す
- ▶ 1方向性関数(逆計算が難しい)を利用
- ▶ RSA暗号(Rivest, Shamir, Adleman)
 - ▶ 合成数の素因数分解の難しさが暗号の強度
- ▶ 処理速度は一般的に慣用暗号より遅い
- ▶ 秘匿化だけでなく署名(認証)にも使える
- ▶ 電子署名だけならハッシュ(Hash)も使える
 - ▶ ハッシュは暗号と違って元に戻らない
 - ▶ 戻らない利点を使って匿名化技術に

▶ 4

情報セキュリティ論 暗号(2) 2020/5/22



4

公開鍵暗号のインパクト

- ▶ 暗号が秘匿化だけでなく認証に使える
- ▶ デジタルなものに電子署名
- ▶ インターネット上でビジネス
- ▶ 慣用暗号と組み合わせると実用的
 - ▶ 鍵の交換は公開鍵
 - ▶ データ伝送時は慣用暗号
- ▶ 数学的な難しさに依存する安心感



▶ 5

情報セキュリティ論 暗号(2) 2020/5/22



帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

5

公開鍵暗号・デジタル署名の基礎

- ▶ 数学的な難しさ
 - ▶ 素因数分解: 合成数を素数分解する難しさ
 - ▶ 素数の判定はランダムアルゴリズムで解ける
- ▶ 1方向性関数
 - ▶ $y=f(x)$ で、 x を与えたとき y は簡単に見つかるが、 y が与えられたとき x を見つけるのは難
 - ▶ $f(\cdot)$ が暗号化で、 $f^{-1}(\cdot)$ が復号化



▶ 6

情報セキュリティ論 暗号(2) 2020/5/22



帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

6

公開鍵暗号の原理(1)暗号通信

- ▶ 初期化
 - ▶ A(Alice)は公開鍵と秘密鍵のペアを生成して、公開鍵は公開鍵簿に登録
- ▶ 暗号化
 - ▶ B(Bob)は公開鍵簿からAの公開鍵を入手し、その鍵で暗号化してAに送る
- ▶ 復号化
 - ▶ Aは自分だけの秘密鍵で復号化する
 - ▶ これができるのはAだけ



▶ 7

情報セキュリティ論 暗号(2) 2020/5/22



7

公開鍵暗号の原理(2)電子署名

- ▶ 初期化
 - ▶ A(Alice)は公開鍵と秘密鍵のペアを生成して、公開鍵は公開鍵簿に登録
- ▶ 署名して送る
 - ▶ Aは自分の秘密鍵で暗号化してB(Bob)に送る
- ▶ 復号化
 - ▶ Bは公開鍵簿からAの公開鍵を見つけ、Aから送られてきたものをAの公開鍵で復号化する
 - ▶ このような伝送文を送れるのはAだけ

▶ 8

情報セキュリティ論 暗号(2) 2020/5/22



8

RSA暗号

- ▶ 1977年MITのRivest, Shamir, Adleman



- ▶ 鍵生成

- ▶ 2つの素数 p, q : $n=p \times q$: $\lambda(n)=\text{LCM}(p-1, q-1)$
- ▶ $Z_{\lambda(n)}$ のある e に対して、 $d=1/e \pmod{\lambda(n)}$
 - ▶ ただし、 $\text{GCD}(e, \lambda(n))=1$
- ▶ 秘密鍵(d または p, q): 公開鍵(e, n)
- ▶ 暗号化: $c=m^e \pmod{n}$
- ▶ 復号化: $m=c^d \pmod{n}$
- ▶ n は200桁程度の数が使われている

▶ 9

情報セキュリティ論 暗号(2) 2020/5/22

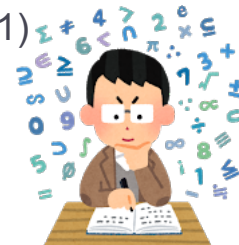
帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

9

RSA暗号(例題)

- ▶ 数学的準備

- ▶ $Z_3 = \{0, 1, 2\}$ 3進数
- ▶ 鍵生成
 - ▶ $p=7, q=11$: $n=p \times q=77$: $\lambda(n)=\text{LCM}(6, 10)=30$
 - ▶ $Z_{\lambda(n)}=\{0, 1, \dots, 29\}$ のある $e=7$ に対して、
 - ▶ $d=1/e \pmod{\lambda(n)}=13$, $\lambda(n)=30$, $7 \times 13 = 91 = 1 \pmod{30}$
 - ▶ ただし、 $\text{GCD}(e, \lambda(n))=\text{GCD}(7, 30)=1$
 - ▶ 秘密鍵(d または p, q) (13または7, 11)
 - ▶ 公開鍵(e, n) (7, 77)
- ▶ $M=\{0, 1, 2, \dots, 76\}$
- ▶ 暗号化: $c=m^7 \pmod{77}$
- ▶ 復号化: $m=c^{13} \pmod{77}$



▶ 10

情報セキュリティ論 暗号(2) 2020/5/22

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

10

その他の公開鍵暗号

- ▶ ナップザック暗号
 - ▶ 破られた公開鍵暗号: 1983年
 - ▶ $1+2+4+8+16+32+64+128=255$
 - ▶ $(01010101) = ?$
- ▶ 楕円暗号: 楕円関数を利用

