暗号技術
ー鍵配送方式と公開鍵暗号方式ー

- 古典的鍵配送方式
- 公開鍵暗号方式
- 耐タンパー装置を用いたIDに基づく暗号方式
- RSA暗号
- DH鍵共有方式とエルガマル暗号
- さまざまな公開鍵暗号方式
- 公開鍵暗号方式の安全性
- 公開鍵暗号で何ができるのか

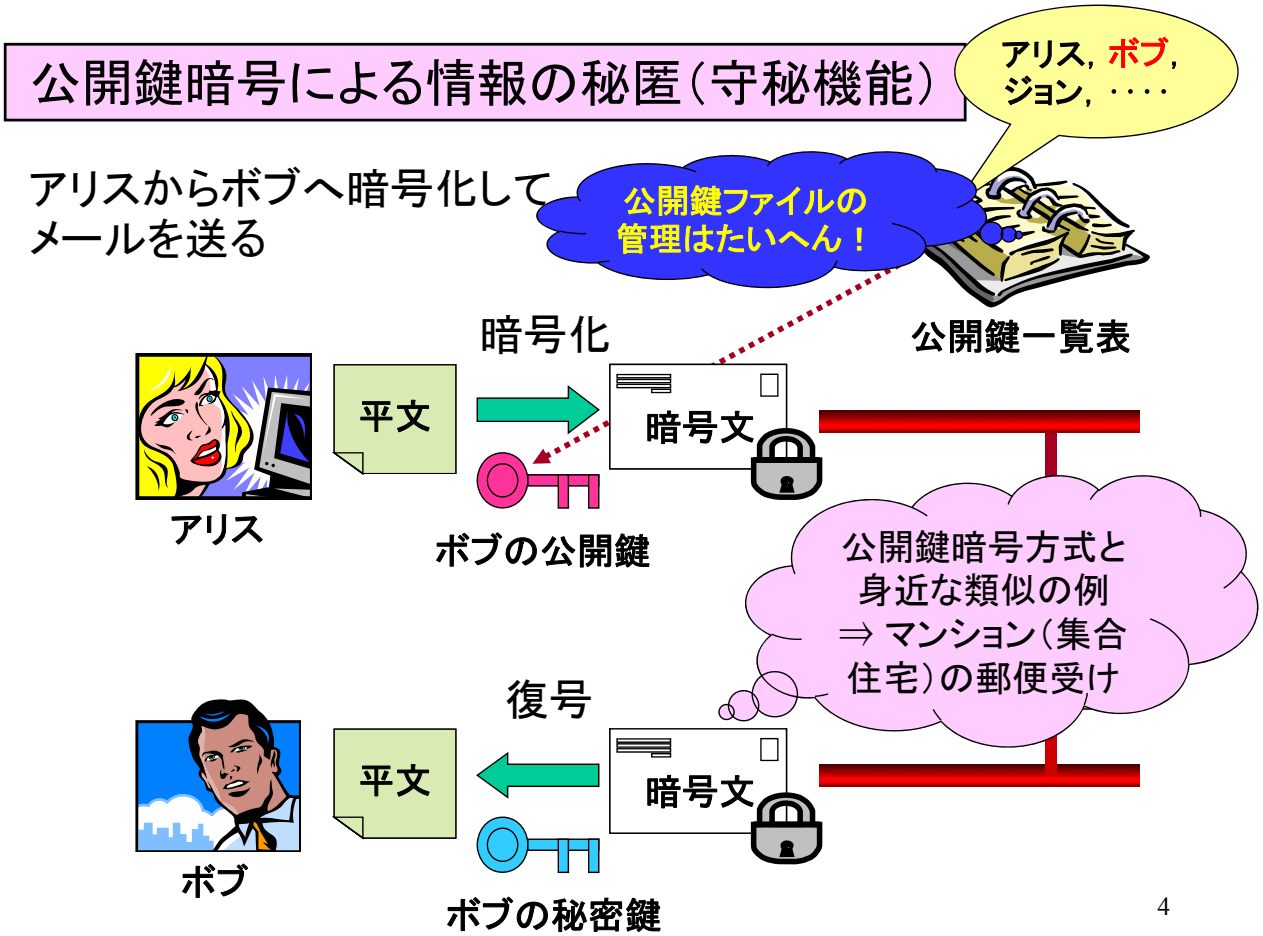
古典的鍵配送方式

- ネットワーク暗号を共通鍵暗号で実現
  ◆リンク暗号　◆エンドーエンド暗号
- 鍵配送問題
- 鍵管理センター ⇒ ネットワークが大規模になるとセンターの負担が大きくなる

公開鍵暗号／複数鍵暗号

- 秘密鍵と公開鍵（暗号鍵≠復号鍵）
  ◆秘密鍵で暗号化、公開鍵で復号
  ◆公開鍵で暗号化、秘密鍵で復号
  ◆公開鍵から秘密鍵を推定するのは現状では困難
  （整数論、楕円関数論など数学の理論で保証）
- 鍵の配送が不要
- 情報の秘匿だけでなく、情報の認証にも使える
- 電子署名（電子印鑑）、電子投票、電子マネー、
  電子商取引（E コマース）での利用
- RSA（Rivest, Shamir, Adelman)暗号、エルガマル暗号、
  楕円曲線暗号、・・・
- 共通鍵暗号に比べて処理が遅い
  ⇒ 共通鍵暗号の鍵だけを公開鍵暗号を使って暗号化する
  (PGPシステム）

公開鍵暗号による情報の秘匿（守秘機能）



耐タンパー装置を用いたIDに基づく暗号方式

- Eメールアドレスなど、ID (Identification) に基づく暗号方式（公開鍵ファイルが不要）
- 耐タンパー装置 ⇒ 秘密鍵の保管、暗号の復号において、不正に情報を読み出したり、書き換えたりするのが難しい装置
- 秘密情報は安全な記憶装置に記憶
- 他人だけでなく、正当な使用者自身に対しても秘密の情報の読み出しや不正な書き換えを許さないような構成にする
- ICカード、スマートカードで実現

クリプテックス（Cryptex）

これも耐タンパー装置の一種

レオナルド・ダ・ヴィンチによる発明といわれている、秘密文書を格納する装置“クリプテックス”

映画“ダ・ヴィンチ・コード”に登場。

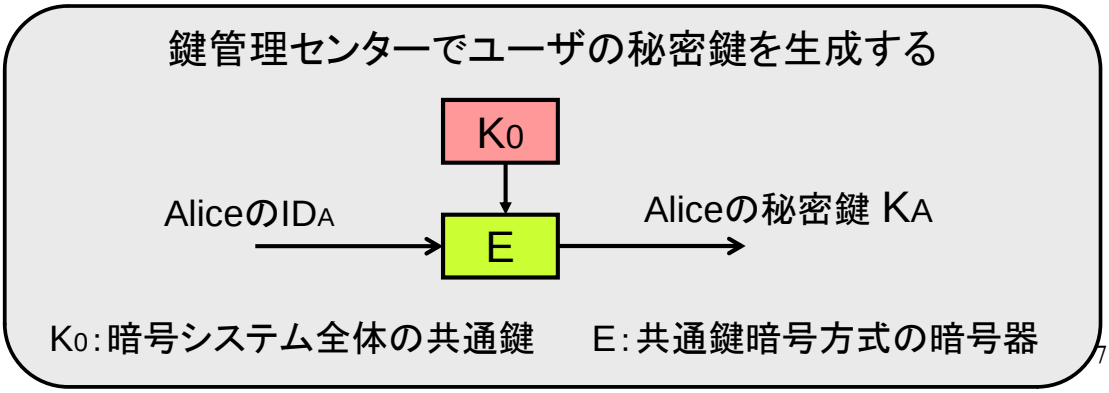
“クリプテックス”も耐タンパー装置の一種と考えられる。

耐タンパー装置を用いたIDに基づく暗号方式

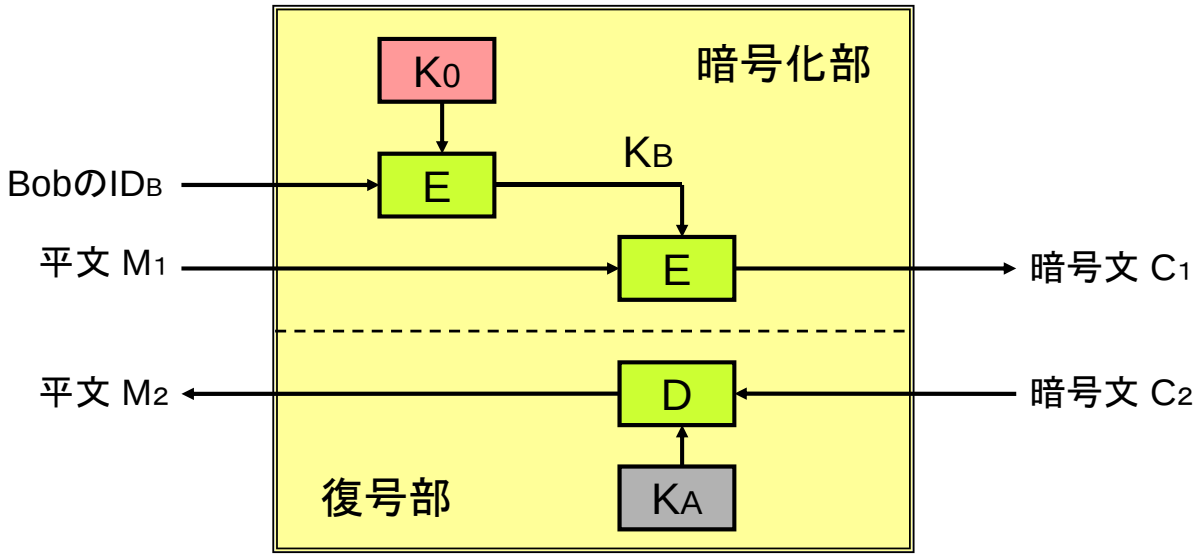
- 安全な共通鍵暗号方式
- 信用できる鍵管理センター

－暗号システム全体の共通鍵の管理（最重要：この鍵が分かるとシステムが破られる）

－最初に各ユーザごとに耐タンパー装置に秘密情報を封じ込めて渡しさえすればよい



耐タンパー装置を用いたIDに基づく暗号方式



Aliceの耐タンパー装置

E：共通鍵暗号方式の暗号器　　D：共通鍵暗号方式の復号器

K0：暗号システム全体の共通鍵

KA：Aliceの秘密鍵（鍵管理センターでAliceのIDAからつくる）

KB：Bobの秘密鍵（耐タンパー装置の中でBobのIDBからつくる）

RSA暗号（R.L.Rivest, A.Shamir, L.Adleman)

Alice の公開鍵・秘密鍵の生成

① Alice は二つの素数 p, q をランダムに選び、その積 $n = pq$ を計算する。

② $k = \mathrm{LCM}(p\text{-}1, q\text{-}1)$（LCM：最小公倍数）を計算し、$k$ と最大公約数が 1 となる正整数 e を一つ選び、**(e , n)** を公開鍵ファイルに Alice の**公開鍵**として登録する。

③ $ed \bmod k = 1$ となる d を計算し、Alice は ***d*** を**秘密鍵**として秘密に保管する。

RSA暗号（R.L.Rivest, A.Shamir, L.Adleman)

Bob から Alice への暗号通信

〔準備〕Bob は平文を 0 以上 n-1 以下の整数列 $M_1, M_2, \cdots, M_i, \cdots$ で表す。以下、$M = M_i$ とおく。

〔暗号化〕Bob は公開鍵ファイルから Alice の公開鍵 (e , n) を調べて、平文 M から $C = M^e \bmod n$ を計算し、C を暗号文として Alice に送る。

〔復号〕Alice は公開鍵 n と秘密鍵 d を用いて、受け取った暗号文 C から $M = C^d \bmod n$ を計算し、平文 M に復号する。

RSA暗号の例

公開鍵・秘密鍵の生成

① $p = 5, q = 11$ とすると $n = pq = 55$ となる。

② $k = \mathrm{LCM}(p-1, q-1) = \mathrm{LCM}(4,10) = 20$ となる。k と最大公約数が 1 となる正整数として $e = 3$ を選ぶ。
$(e,n)=(3,55)$ を公開鍵とする。

③ $ed \bmod k = 3d \bmod 20 = 1$ より $d = 7$ を秘密鍵とする。

暗号通信

〔暗号化〕平文を $M = 4$ とすると暗号文 C は以下のようになる。

$$C = M^e \bmod n = 4^3 \bmod 55 = 64 \bmod 55 = 9$$

〔復号〕暗号文を $C = 9$ とする。以下の計算により平文 M=4 に復号される。

$$M = C^d \bmod n = 9^7 \bmod 55$$
$$= 4782969 \bmod 55 = 4$$

RSA暗号の安全性

一方向性関数
「順変換は簡単、しかし逆変換は困難」という仕掛け

秘密鍵を求めるには、合成数 n を素数 p と q の積に素因数分解しなければならない。しかし、p , q が非常に大きな素数の場合、n を $p \times q$ の形に素因数分解するのは大変難しい！

【素因数分解問題】 次の数を素因数分解せよ

(a) 504233 (b) 2077003 (c) 71255441

n の桁数とRSA暗号の安全性
1990年代：512ビット（10進数155桁）
⇒ 現在：1024ビット（10進数309桁）

DH（ディフィ・ヘルマン）鍵共有方式とエルガマル暗号

離散対数問題の難しさを利用

RSA暗号と並んで実用的な暗号

離散対数問題

p を 3 以上の素数とし、a と y を p-1 以下の正の整数とするとき、$y = a^x \bmod p$ を満たす x を求めるという問題 。
（x を y の離散対数という。）

（例）p =11, a =2, y =10 のとき、$2^x \bmod 11 = 10$ を満たす x を求めよ。（答）x =5（11の離散対数は5）

p が10進数300桁程度（1024ビット程度）であれば、べき乗剰余 y の計算は簡単、逆に、離散対数 x の計算は困難
（⇒ 一方向性関数）

さまざまな公開鍵暗号方式

- ラビン（Rabin）暗号・・・大きな整数の素因数分解の難しさを利用
- マクリース（McEliece）暗号・・・誤りを訂正する符号の復号の難しさを利用
- MI（松本・今井）暗号・・・多変数多元連立方程式を解く難しさを利用
- 楕円曲線暗号・・・楕円曲線上の離散対数問題の難しさを利用。公開鍵や秘密鍵の長さを10進数50桁程度（160ビット程度）としても、現状では十分に安全。（RSA暗号やエルガマル暗号に比べて鍵の長さを1／6以下にできる！）

公開鍵暗号で何かできるのか

守秘機能

	秘密鍵の配送（共有）問題	暗号化・復号化の計算量
共通鍵暗号方式	あり	小
公開鍵暗号方式	なし	大

ハイブリッド暗号

「公開鍵方式を用いて、共通鍵方式の秘密鍵（共通鍵）を送り、伝送すべき情報は共通鍵暗号で送る。」

認証機能

ディジタル署名と認証方式
⇒公開鍵ファイルの管理問題の解決

ハイブリッド暗号