前回： 素数判定・素因数分解のアルゴリズム

- **素数判定**
  - ⋆ **Fermat テスト**
  - ⋆ **Agrawal-Kayal-Saxena の**
    多項式時間アルゴリズム

- **素因数分解**
  (多項式時間アルゴリズムは知られていない)
  - ⋆ **二次篩法**
  - ⋆ **数体篩法　　等々**

素因数分解問題の高速なアルゴリズムの発見

⇓

RSA 暗号の解読

しかし、逆は真とは限らない

(解読には色々な方法があり得る)

「何で負けても負けは負け」

素因数分解問題の高速なアルゴリズムの発見

$\Downarrow$

RSA 暗号の解読

しかし、逆は真とは限らない

(解読には色々な方法があり得る)

「何で負けても負けは負け」

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**

$\longrightarrow$ **離散対数問題の利用**

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**

$\longrightarrow$ **離散対数問題の利用**

離散対数問題 (Discrete Logarithm Problem)

p：素数

$g \in \mathbb{Z}$ を 1 つ取って固定

a を与えたとき、

$x \equiv g^a \pmod{p}$ の計算は容易だったが、逆に、

問題：x を与えたとき、

$$g^a \equiv x \pmod{p}$$

を満たす a を見出せ。

離散対数問題 (Discrete Logarithm Problem)

p：素数

$g \in \mathbb{Z}$ を 1 つ取って固定

a を与えたとき、

$x \equiv g^a \pmod{p}$ の計算は容易だったが、逆に、

問題：x を与えたとき、

$$\boxed{g^a \equiv x \pmod{p}}$$

を満たす a を見出せ。

Diffie-Hellman 鍵共有 (key-exchange)

離散対数問題 (DLP) の困難さを利用して、
公開通信路で秘密裡に鍵共有を行なう方式

p : 素数

$1 \leq K \leq p-1$ なる整数 $K \in \mathbb{Z}$ の一つを
公開通信路で秘密裡に共有したい

p と互いに素な整数 $g \in \mathbb{Z}$ を 1 つ取って固定
($g \bmod p$ の位数が充分大きいように選んでおく)

A, B 両者が ランダム かつ 秘密裡に
それぞれ a, b を選ぶ

Diffie-Hellman 鍵共有 (key-exchange)

離散対数問題 (DLP) の困難さを利用して、
公開通信路で秘密裡に鍵共有を行なう方式

p : **素数**

$1 \leq K \leq p-1$ **なる整数** $K \in \mathbb{Z}$ **の一つを**
公開通信路で秘密裡に共有したい

p **と互いに素な整数** $g \in \mathbb{Z}$ **を** 1 **つ取って固定**
($g \bmod p$ **の位数が充分大きいように選んでおく)**

A, B 両者が ランダム かつ 秘密裡に
それぞれ a, b **を選ぶ**

Diffie-Hellman 鍵共有 (key-exchange)

離散対数問題 (DLP) の困難さを利用して、
公開通信路で秘密裡に鍵共有を行なう方式

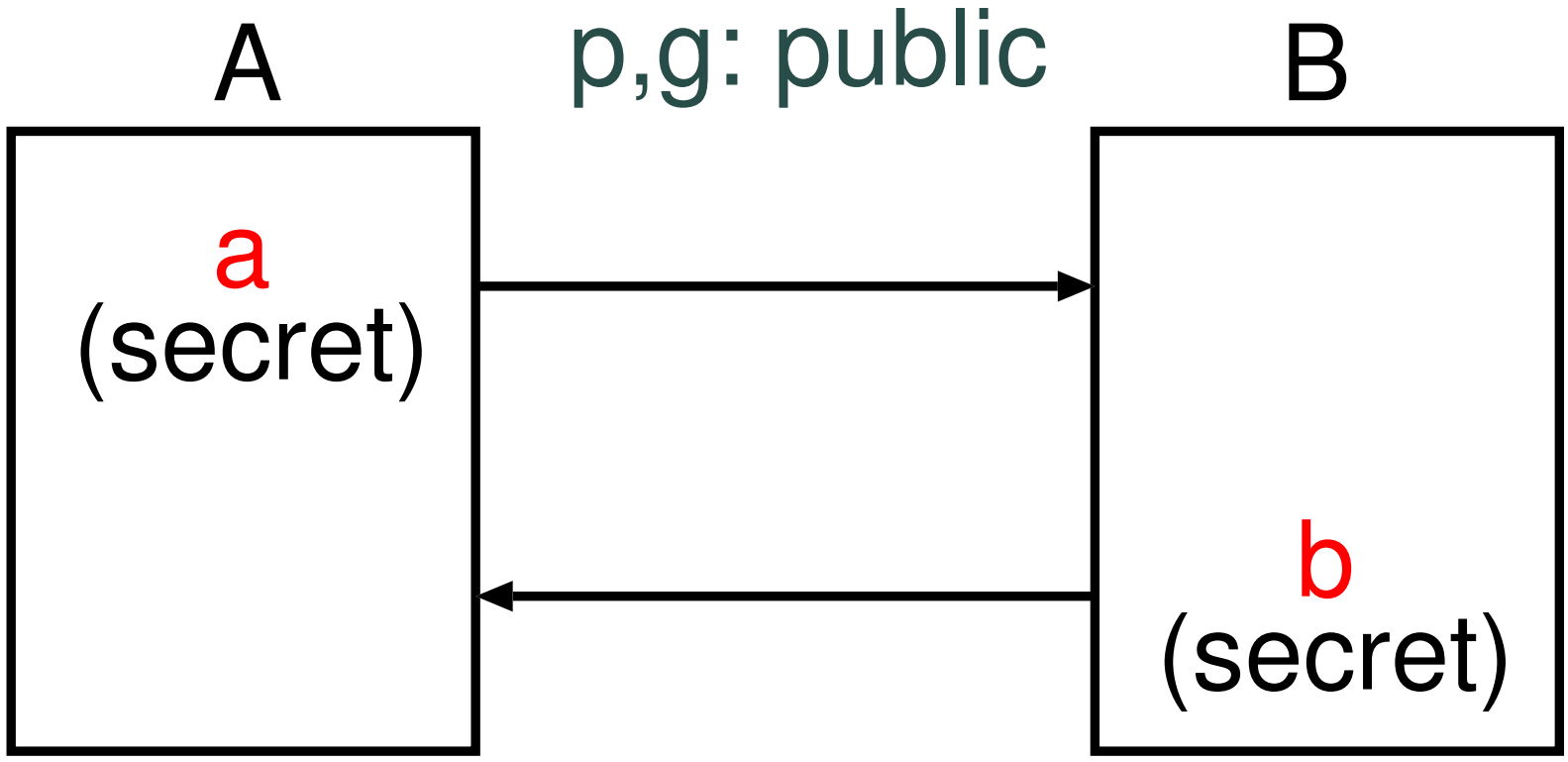
p : **素数**

$1 \leq K \leq p-1$ **なる整数** $K \in \mathbb{Z}$ **の一つを**
公開通信路で秘密裡に共有したい

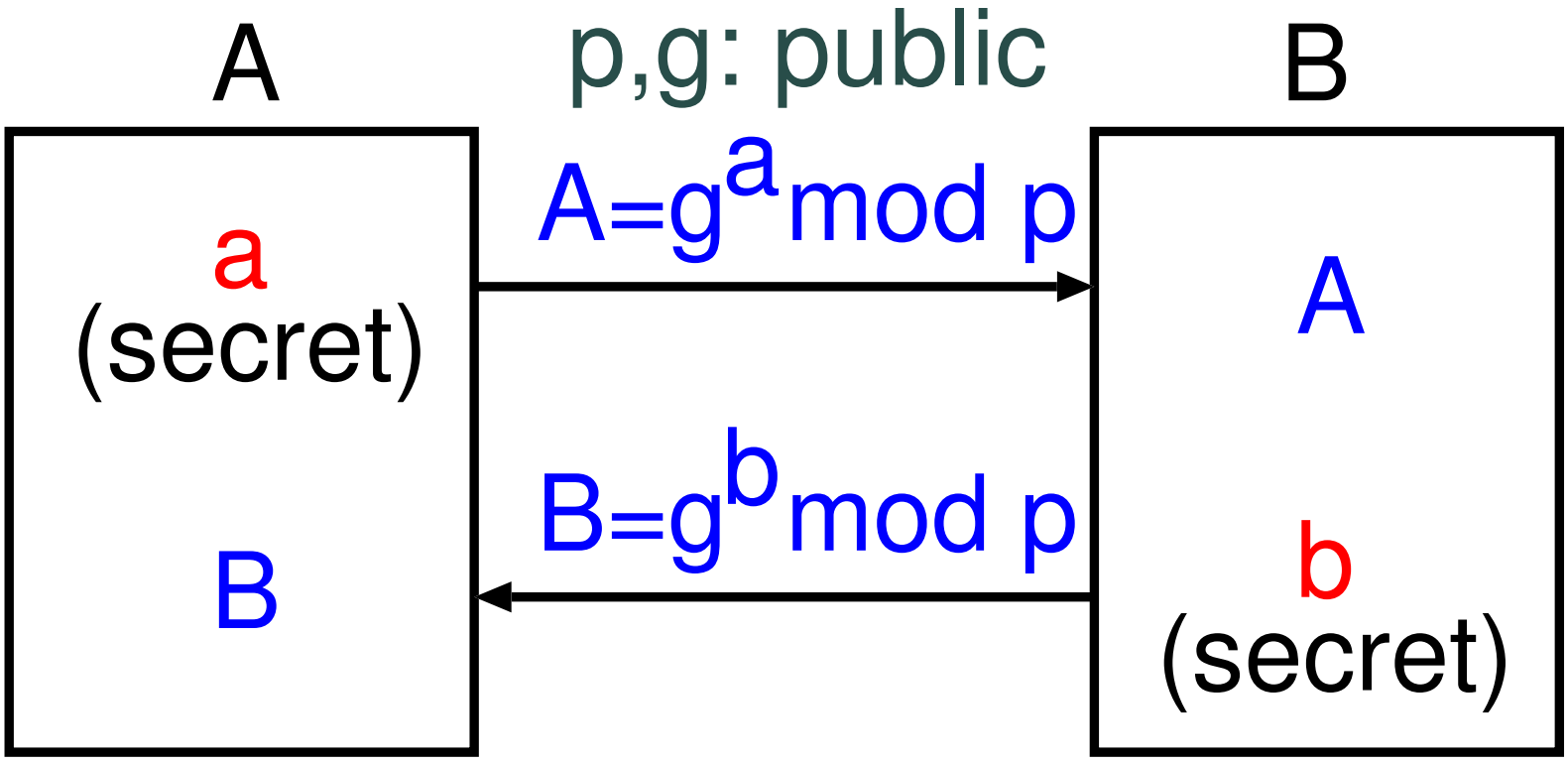
p **と互いに素な整数** $g \in \mathbb{Z}$ **を** 1 **つ取って固定**
($g \bmod p$ **の位数が充分大きいように選んでおく)**

A, B 両者が ランダム かつ 秘密裡に
それぞれ a, b **を選ぶ**

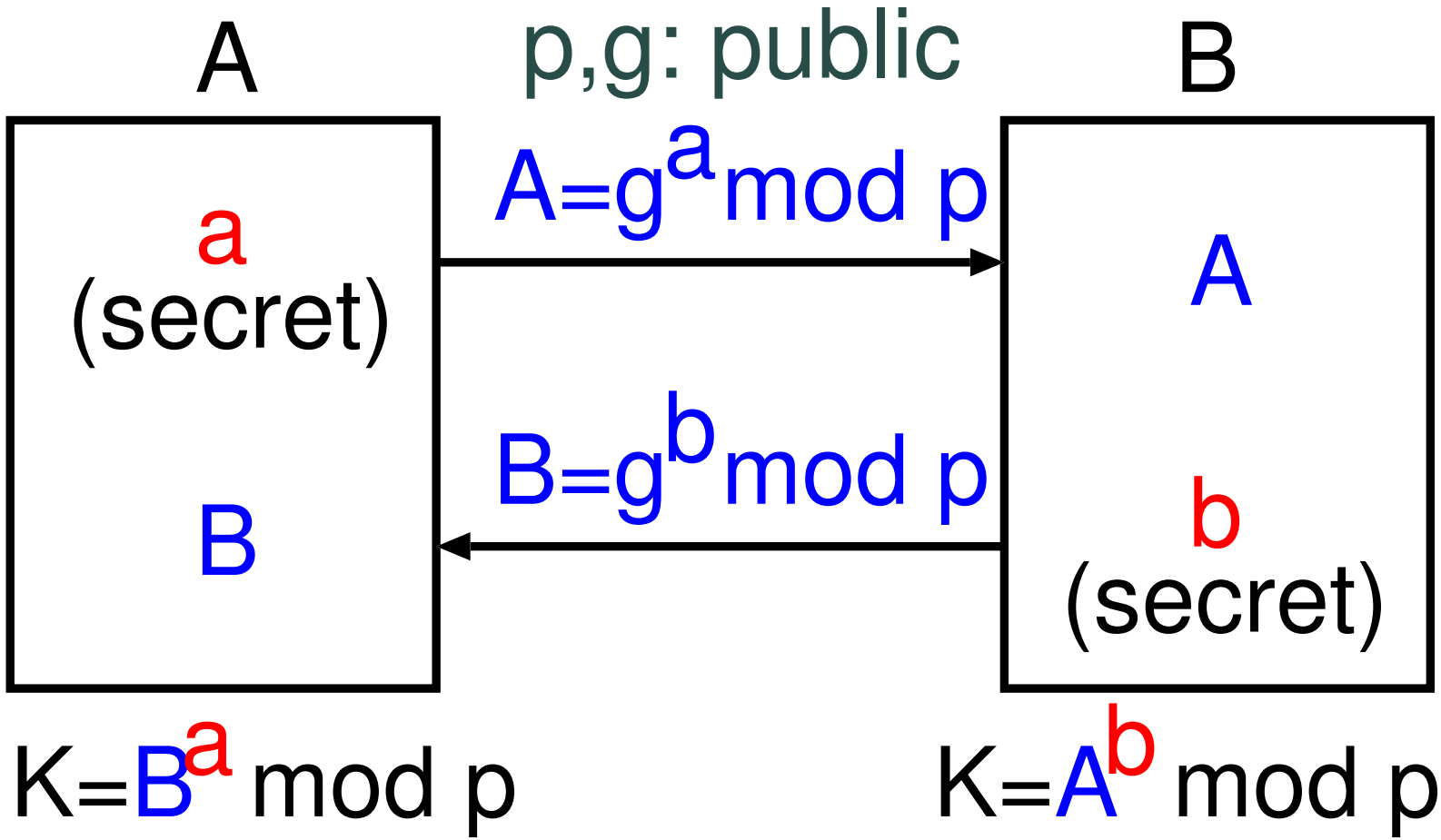
Diffie-Hellman 鍵共有 (key-exchange)



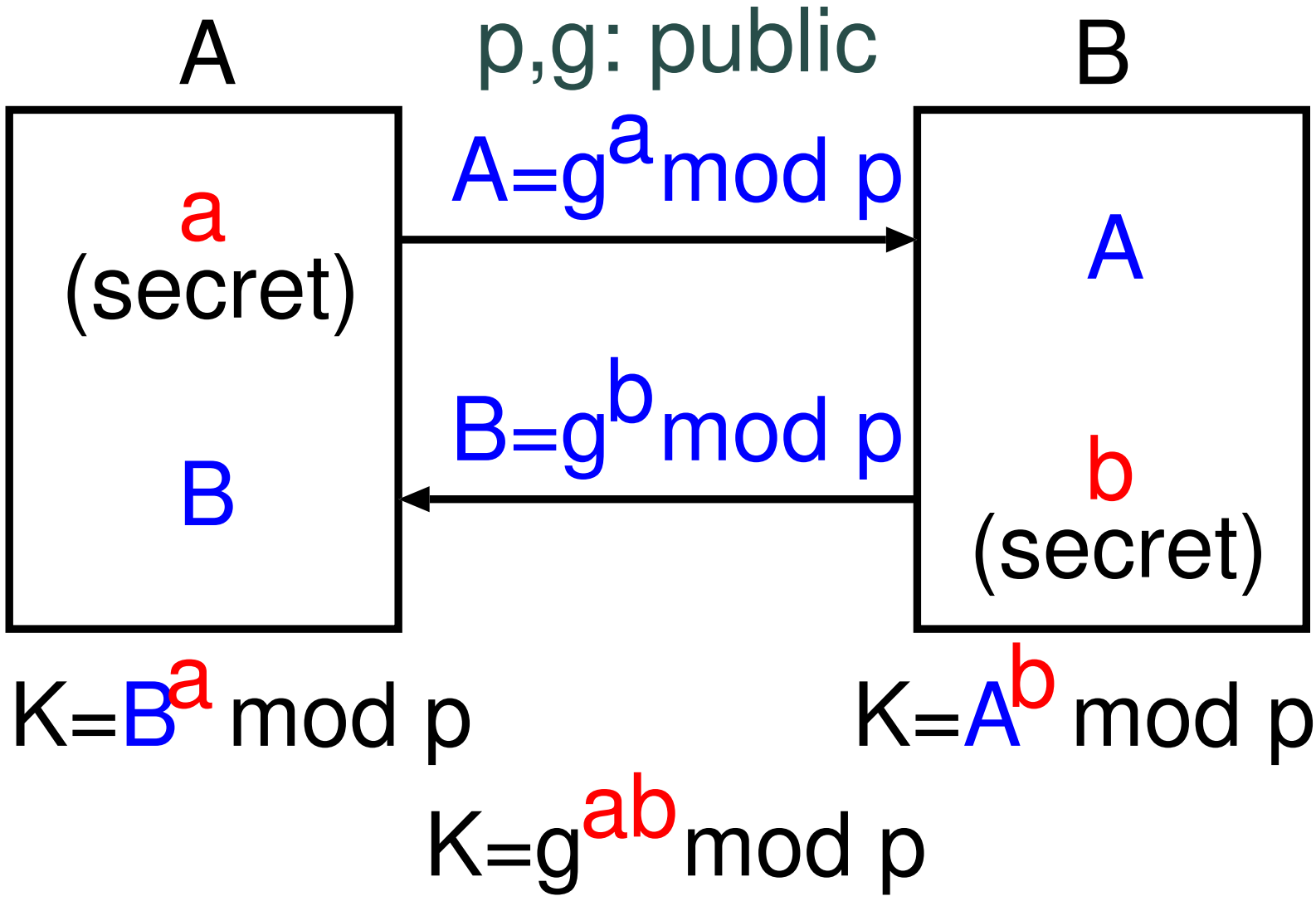
Diffie-Hellman 鍵共有 (key-exchange)



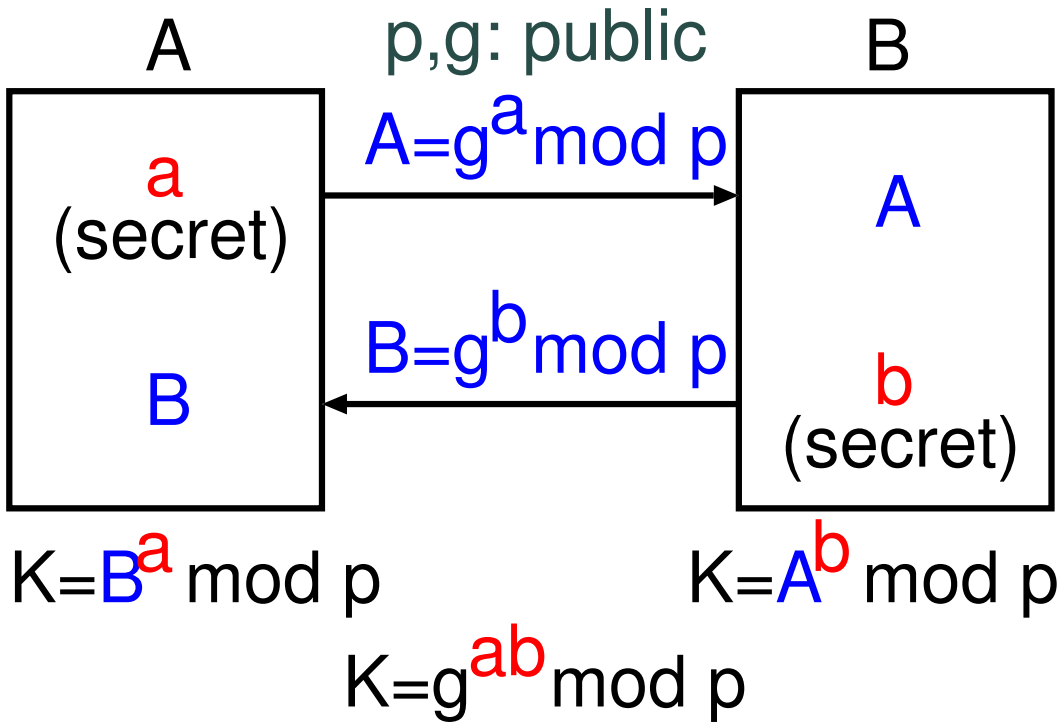
Diffie-Hellman 鍵共有 (key-exchange)



Diffie-Hellman 鍵共有 (key-exchange)



Diffie-Hellman 鍵共有 (key-exchange)



$(\mathrm{p}, \mathrm{g}, \mathrm{A}, \mathrm{B})$ **が判っても** a, b **が判らない (DLP)**

$\longrightarrow$ **秘密鍵** K **の共有が可能 !!**

ElGamal 暗号 (ElGamal encryption system)

離散対数問題 (DLP) を利用し、
乱数を用いた暗号方式

p **：素数**

p **と互いに素な整数** $g \in \mathbb{Z}$ **を** 1 **つ取って固定**
($g \bmod p$ **の位数が充分大きいように選んでおく)**

平文 $M \bmod p$ **を A から B へ送りたい**

ElGamal 暗号 (ElGamal encryption system)

(p, g) : **公開鍵**

$M \bmod p$: **平文**

受信者 B が b **を** ランダム **かつ** 秘密裡に **選ぶ**

$\longrightarrow B := g^b \bmod p$ **を公開**

送信者 A が a **を** ランダム **かつ** 秘密裡に **選ぶ**

$\longrightarrow A := g^a \bmod p,\ C := B^a M \bmod p$ **を送信**

受信者 B は $M = (A^b)^{-1} C \bmod p$ **によって復号**

ElGamal 暗号 (ElGamal encryption system)

(p, g) : **公開鍵**

$M \bmod p$: **平文**

受信者 B が b **を** ランダム **かつ** 秘密裡に **選ぶ**
$\longrightarrow B := g^b \bmod p$ **を公開**

送信者 A が a **を** ランダム **かつ** 秘密裡に **選ぶ**
$\longrightarrow A := g^a \bmod p,\ C := B^a M \bmod p$ **を送信**

受信者 B は $M = (A^b)^{-1} C \bmod p$ **によって復号**

ElGamal 暗号 (ElGamal encryption system)

平文 $\mathrm{M} \longrightarrow$ **暗号文** (A, C)

- **送信データ長が** 2 **倍 (メッセージ膨張)**
- **乱数により、同じ文書が毎回異なる暗号化**

疑似乱数 (pseudorandom number)

充分ランダムに 見える 長い周期の数列を 発生させるアルゴリズム

"Mersenne Twister" (松本-西村、松本-斎藤)
$\cdots$ 現在、事実上最強のアルゴリズム

- MT19937:
  - ⋆ 極めて長周期 (周期 $2^{19937}-1$)
  - ⋆ 極めてランダム (623 次元均等分布)
  - ⋆ 極めて高速
- 本来は Monte-Carlo simulation 用
- 暗号には適切なハッシュ関数と組合わせる

疑似乱数 (pseudorandom number)

充分ランダムに 見える 長い周期の数列を
発生させるアルゴリズム

“Mersenne Twister” (松本-西村、松本-斎藤)
. . . 現在、事実上最強のアルゴリズム

- **MT19937:**
  - ⋆ **極めて長周期 (周期 $2^{19937}-1$)**
  - ⋆ **極めてランダム (623 次元均等分布)**
  - ⋆ **極めて高速**
- **本来は Monte-Carlo simulation 用**
- **暗号には適切なハッシュ関数と組合わせる**

疑似乱数 (pseudorandom number)

充分ランダムに 見える 長い周期の数列を
発生させるアルゴリズム

“Mersenne Twister” (松本-西村、松本-斎藤)
. . . 現在、事実上最強のアルゴリズム

- **MT19937:**
  - ⋆ **極めて長周期 (周期 $2^{19937}-1$)**
  - ⋆ **極めてランダム (623 次元均等分布)**
  - ⋆ **極めて高速**
- **本来は Monte-Carlo simulation 用**
- **暗号には適切なハッシュ関数と組合わせる**

離散対数問題を利用した方式は
他の有限アーベル群でも可能

- 有限体上の楕円曲線の有理点の群
  (楕円曲線暗号)
- 有限体上の超楕円曲線の Jacobian の有理点の群
  (超楕円曲線暗号)
- 代数体の ideal 類群