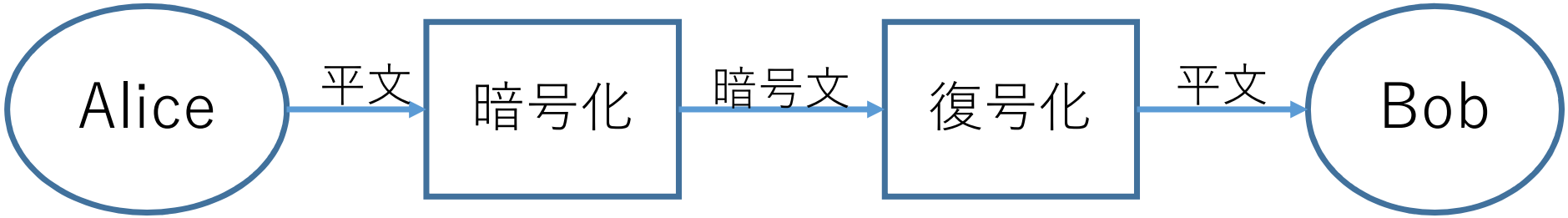
# 公開鍵暗号

公開鍵暗号は、暗号化鍵と復号化鍵が異なっている非対称な暗号系である。公開鍵暗号は、暗号システムにおける鍵配送の問題を解決することができ、また、公開鍵暗号のしくみを利用することで電子署名を実現することもできる。このため、公開鍵暗号は現在の情報化社会において必要不可欠な技術となっている。

# RSA暗号

- 1978年にRivest、Shamir、Adlemanによって考案された公開鍵暗号。
- 最初に考案された公開鍵暗号であり、現在も最も広く利用されている
- 素因数分解の困難性を利用して構築されている
- 鍵サイズは、現在、2048bit以上（最低でも1024bit）が推奨されている




- 以下では、Aliceが平文Mを暗号化して暗号文Cを作り、Bobに送る。BobはCを復号して平文Mを得るものとする。

# RSA暗号（準備）

- Bob（受信者）が準備を行う

1. ２つの異なる大きな素数$p,q$を準備する
2. 法$N = pq$を計算する
3. オイラーの関数の値$\varphi(N) = (p-1)(q-1)$を求める
4. 上で求めた$\varphi(N)$と互いに素な数$e$を任意に決める
5. 数$d$を$ed = 1 \pmod{\varphi(N)}$を解いて求める

- Bobは、数$N, e$を公開鍵として公開する（Aliceに伝える）
- Bobは、数$p, q, d$を秘密鍵として秘密に保管しておく

（注）素数$p, q$や鍵$e, d$の選び方によっては暗号強度が低下することがあるが、ここでは省略する。

# RSA暗号（暗号化と復号化）

- 暗号化（Aliceが行う）

1. 平文$M(0 \leq M < N)$を準備する
2. 暗号文$C$を$C = M^e \pmod N$により計算する

- 復号化（Bobが行う）

1. 暗号文$C$を受信する
2. 平文$M$を$M = C^d \pmod N$により計算する

- （注）公開鍵$(N, e)$は公開されているので暗号化は誰でも可能だが、復号化は秘密鍵を知っているBobだけが行える

# RSA暗号の原理

- 暗号文が復号できる理由（$(M,N)=1$とする）
  暗号文$C=M^e \pmod N$を復号の式に代入する
  $$C^d=M^{ed}$$
  ここで、$ed=1 \pmod{\varphi(N)}$なので、$ed=t\varphi(N)+1$（$t$:整数）
  とおける。従って、
  $$M^{ed}=M^{t\varphi(N)+1}=M^{t\varphi(N)}\times M^1 \pmod N$$

となる。オイラーの定理より、$M^{\varphi(N)}=1(mod\ N)$なので、結局

$$C^d=M^{ed}=M \pmod N$$

- $(M,N)\neq 1$の時は、$M=0 \pmod p$か$M=0 \pmod q$のいずれかなので、mod $p$とmod $q$に分けて考えることにより、やはり
  $C^d=M \pmod N$がいえる

# RSA暗号の鍵の導出について

- RSA暗号の準備のステップ5において、$ed = 1\ (mod\ \varphi(N))$を解いて$d$を求めたが、実際には$\varphi(N)$の代わりに$LCM(p-1, q-1)$を用いる。
- なぜなら、$a^{p-1} = 1\ (mod\ p)$かつ$a^{q-1} = 1(mod\ q)$であるから、$a^{LCM(p-1,q-1)} = 1(mod\ N)$が成り立つからである。
- $LCM(p-1, q-1) < \varphi(N)$であるので、より小さい最小公倍数を法にするほうが計算が楽

# RSA暗号と素因数分解の関係

- RSA暗号を復号するために必要なパラメータは$N$と$d$だが、$N$は公開鍵なので$d$が分かれば復号できる。$d$は、
$$ed = 1 \pmod{\varphi(N)}$$
を解いて求めるので、$\varphi(N) = (p-1)(q-1)$の値が分かればよい。しかし、この値は、$N$の素因数分解が分からなければ求められない。
- 明らかに、法 $N$ が素因数分解できればRSA暗号は解読できるが、素因数分解以外の方法でRSA暗号が解読できるのかどうかは証明されていない（素因数分解とRSA暗号の解読問題が同値かどうかは分かっていない）
- 素因数分解と解読問題が同値であることが証明されている公開鍵暗号としてRabin（ラビン）暗号が知られている。

# RSA暗号（例）

- （準備）

1. 素数$p = 3, q = 11$とする
2. 法$N = pq = 33$
3. オイラーの関数$\varphi(N) = 2 \times 10 = 20$
   （あるいは、$LCM(2,10) = 10$）
4. 上で求めた$\varphi(N) = 20$と互いに素な$e = 3$を選ぶ
   （あるいは、$LCM(2,10) = 10$と互いに素な$e = 3$を選ぶ）
5. 一次合同式$ed = 1(\mathrm{mod}\ \varphi(N))$を解いて、$d = 7$
   （あるいは、$ed = 1(mod\ LCM(2,10))$を解いて$d = 7$）

- 公開鍵$(N, e) = (33,3)$、秘密鍵$(p, q, d) = (3,11,7)$となる

# RSA暗号（例、続き）

- （暗号化）

1. 平文$M = 5$とする
2. 暗号文$C = M^e = 5^3 (\mathrm{mod}\ 33) = 26 (\mathrm{mod}\ 33)$

- （復号化）

1. 暗号文$C = 26$を受信する
2. 平文$M = C^d = 26^7 (\mathrm{mod}\ 33) = 5 (\mathrm{mod}\ 33)$

# 高速指数演算法

- RSA暗号をはじめ、多くの暗号ではべき乗の計算が必要
  →高速にべき乗計算を行う必要がある
- （例）$M^{11}$を計算する時、普通に計算すると$M^{11} = M \times M \times \cdots \times M$となり、10回の乗算が必要。
- しかし、11は2進数表現で、1011と書けることに注意すると、
  $$M^{11} = (M^2 \times M^2)^2 \times M^2 \times M$$
  であるので、５回の乗算で計算できる
- なぜなら、(1)$M^2$を計算（乗算1回）、(2)$M^4 \leftarrow M^2 \times M^2$を計算（乗算1回）、(3)$M^8 \leftarrow M^4 \times M^4$を計算（乗算1回）、(4)$M^{11} \leftarrow M^8 \times M^2 \times M$を計算（乗算2回）で計算できるからである
- 一般に、$M^e$を計算する時、高々$2\lfloor \log_2 e \rfloor$回の2乗演算と乗算で計算できる。

# RSA暗号の復号の高速化

- 受信者は法$N$の素因数$p, q$を知っているので復号を高速化できる

1. $d_1 = d(mod\ p-1), d_2 = d(mod\ q-1)$を（あらかじめ）計算しておく。
2. 暗号文$C$から$C_1 = C(mod\ p), C_2 = C\ (mod\ q)$を求める。
3. $M_1 = C_1^{d_1}(mod\ p), M_2 = C_2^{d_2}(mod\ q)$を計算する。
4. $\begin{cases} M = M_1(mod\ p) \\ M = M_2(mod\ q) \end{cases}$を解いて、平文$M$を求める

- 素因数$p, q$は法$N$の約半分のサイズなので全体で4～8倍の高速化が可能

# Rabin暗号

- （準備）Bobが行う

1. ２つの異なる大きな素数$p, q$を準備する
2. 法$N = pq$を計算する
3. 法$N$を公開する（Aliceに伝える）

- （暗号化）Aliceが行う

1. 平文$M(0 \leq M < N)$を準備する
2. 暗号文$C = M^2 (\mathrm{mod}\ N)$を計算する
3. 暗号文$C$をBobに送る

# Rabin暗号（復号化）

- （復号）Bobが行う

1. 二次合同式$m^2 = C(\mathrm{mod}\, p)$を解き、解を$a_1, a_2$とする。同様に$m^2 = C(\mathrm{mod}\, q)$を解き、解を$b_1, b_2$とする。
2. 連立一次合同式$\begin{cases} M = a_1(\mathrm{mod}\, p) \\ M = b_1(\mathrm{mod}\, q) \end{cases}$、$\begin{cases} M = a_1(\mathrm{mod}\, p) \\ M = b_2(\mathrm{mod}\, q) \end{cases}$、$\begin{cases} M = a_2(\mathrm{mod}\, p) \\ M = b_1(\mathrm{mod}\, q) \end{cases}$、$\begin{cases} M = a_2(\mathrm{mod}\, p) \\ M = b_2(\mathrm{mod}\, q) \end{cases}$をそれぞれ解く
3. 上記２の４つの解のうち、いずれか一つが正しい平文Mである

- １の2次合同式は法が素数の場合は効率よく解く方法が知られている
- ３で正しいMを選ぶ方法は、平文が自然言語（日本語など）であれば意味をもつ文章になっているかどうかで判断できる。または、平文Mにあらかじめ何らかのチェック用コードを付加しておけばよい

# Rabin暗号（例）

- 素数$p = 5, q = 7$とする。法$N = p \times q = 35$である。$M = 11$とする
- （暗号化）暗号文$C = M^2 = 11^2 = 16 \pmod{35}$
- （復号化）$m^2 = 16 \pmod{5}$を解くと（$m = 0,1,\cdots,4$を代入して求めればよい）、$m = 1 \text{ or } 4$。同様に$m^2 = 16 \pmod{7}$を解いて、$m = 3 \text{ or } 4$。従って、以下の4つの連立一次合同式を解く。
  $\begin{cases} M = 1 \pmod{5} \\ M = 3 \pmod{7} \end{cases}'$ $\begin{cases} M = 1 \pmod{5} \\ M = 4 \pmod{7} \end{cases}'$ $\begin{cases} M = 4 \pmod{5} \\ M = 3 \pmod{7} \end{cases}'$ $\begin{cases} M = 4 \pmod{5} \\ M = 4 \pmod{7} \end{cases}$
  これらの解は、31、11、24、4であり、この場合は2番目が正しい平文である。

# 巡回乗法群と原始元

- $y = 2^x \pmod{11}$を考える

| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| y | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

→元2は10乗すると初めて1になる（べき乗により1～10の元が全て現れる）
このような元を原始元（または生成元）と呼ぶ

- $y = 5^x \pmod{11}$の場合

| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| y | 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 |

→元5は5乗すると1になる（べき乗しても1～10の全ての元は現れない）
元5は原始元ではないことがわかる

# 離散対数問題

- 素因数分解問題とならび、現実的な時間で解くことが困難な問題。多くの暗号で用いられる。
- 大きな素数$p$を法とするべき乗算を考える。ある数$g(0 < g < p)$について、$g$を$p-1$乗した時に初めて1になるとき、$g$を法$p$における原始元（または生成元）と呼ぶ（原始元は必ず存在することが証明できる）
- 原始元$g$に対して、$y = g^x \pmod p$を考えるとき$(0 < x < p-1)$、$x$から$y$を求める計算は容易だが、$y$から$x$を求める計算は現実的な時間で解く方法が知られていない。この問題は離散対数問題と呼ばれている。

# ElGamal暗号（エルガマル暗号）

- 離散対数問題の困難さに基づく公開鍵暗号
- （準備）大きな素数$p$、法$p$における原始元$g$を用意する。秘密鍵$s(1 \leq s < p-1)$を選び、$y = g^s \pmod p$を求める。公開鍵は$(p, g, y)$、秘密鍵は$s$である。
- （暗号化）平文$M(0 \leq M < p)$とする。乱数$k(0 < k < p-1)$を選び、$R = g^k \pmod p$および、$C = y^k M \pmod p$を計算する。暗号文は$(R, C)$である。
- （復号化）暗号文$(R, C)$から、$R^{-s}C = g^{-ks}g^{sk}M = M \pmod p$により平文$M$を計算する。
- （注）乱数$k$は毎回変更する必要がある（なぜか考えてみよ）

# Elgamal暗号（例）

- （準備）素数$p = 11$、原始元$g = 2$、秘密鍵$s = 8$とする。
  $y = g^s = 2^8 = 3 (\mathrm{mod}\ 11)$となる。公開鍵$(p, g, y) = (11,2,3)$である。
- （暗号化）平文$M = 5$とする。乱数$k = 6$とする。

$$R = g^k = 2^6 = 9 (\mathrm{mod}\ 11)$$
$$C = y^k M = 3^6 \times 5 = 3 \times 5 = 4 (\mathrm{mod}\ 11)$$

  暗号文$(R, C) = (9,4)$である。
- （復号化）$M = R^{-s} C = 9^{-8} \times 4 = 9^2 \times 4 = 4 \times 4 = 16 = 5 (\mathrm{mod}\ 11)$と復号できる。なお、フェルマーの小定理より$9^{10} = 1 (\mathrm{mod}\ 11)$なので、$9^{-8} = 9^2 (\mathrm{mod}\ 11)$を使った。