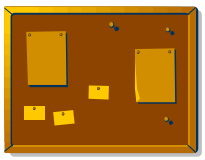
[RSA 暗号の仕組み]

公開掲示板



(Bob, n, e), ... : ユーザと公開鍵のリストの一覧

[Step 3]

Bob の公開鍵(n, e)を入手

[Step 2]

Bob は鍵の一部(n, e)を登録(公開鍵)

送信者 Alice

受信者 Bob

[Step 1] 準備 (鍵の生成) :

・素数 p, q を設定(300 桁以上が推奨);

・ $n = pq$ (n: p, q の積) を計算;

・ $ed \div (p-1)(q-1) = S \cdots 1$

となる整数 e, d を設定;

(注: p, q, d は秘密にしておく)

[Step 4] 暗号化:

メッセージ M

$(M \in \{0, 1, 2, \ldots, n-1\})$

$\Rightarrow M^e \div n = T \cdots C$

(C: M の暗号文)

[Step 5]

C を送信

[Step 6] 復号:

$C^d \div n = U \cdots M'$

このとき, 整数の性質より

$M = M'$ となり, メッセージを得る

注 : p, q がわかる(因数分解ができる)と, 復号の際に用いるdの値が容易に計算でき, RSA 暗号は解読されます.