现代密码学

第三十五讲 RSA加密算法

信息与软件工程学院

RSA公钥密码体制历史

麻省理工学院Ron Rivest、Adi Shamir和Leonard Adleman于1978年一起提出RSA加密算法，并受到广泛关注。

RSA公钥密码体制历史

Published in： Communications of the ACM

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

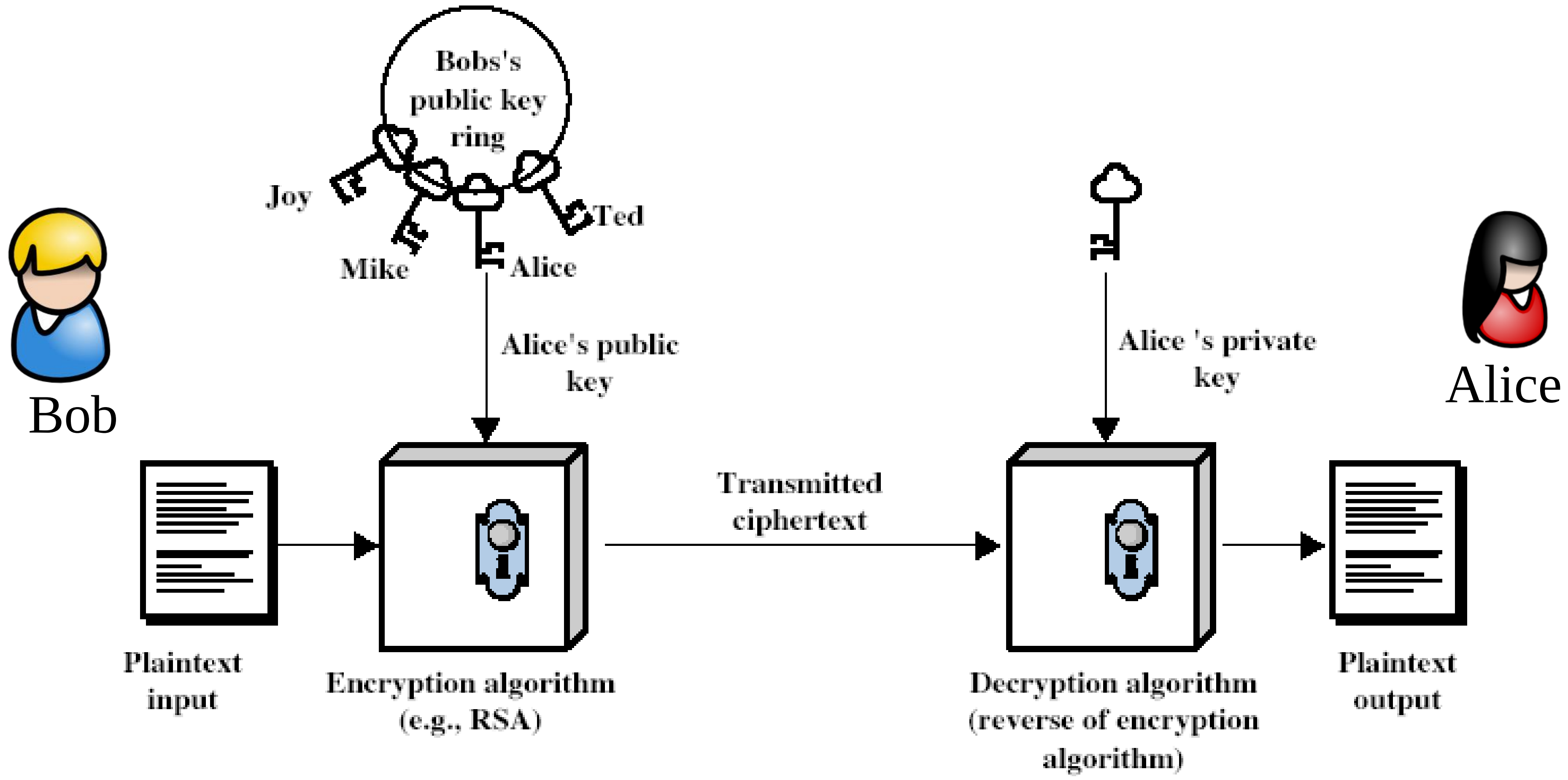
RSA公钥密码体制历史

为奖励Ron Rivest、Adi Shamir和Leonard Adleman发明RSA公钥算法，2002年度美国计算机协会(ACM)为三位学者颁发图灵奖Turing Award。

RSA公钥密码体制历史

RSA目前被广泛应用及部署到不同的场景，比如HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer，是以安全为目标的HTTP通道，简单讲是HTTP的安全版）

公钥密码体制的基本思想



RSA公钥加密体制原理

密钥生成：

1. 选择两个大素数p, q 。（例如：每个1024位）
2. 计算 $n = pq$ ，$z = (p-1)(q-1)$ 。
3. 随机选取e（其中$e < n$），e 与 z 没有公因数。（e, z “互为质数”）
4. 选取 d 使得 $ed - 1$ 能够被 z 完全整除。（换言之：$ed \mod z = 1$ ）
5. 公钥是$\underbrace{(n, e)}_{K_B^+}$ 。私钥是$\underbrace{(n, d)}_{K_B^-}$ 。

RSA公钥加密体制原理

加密/解密算法：

如上所述给出 (n, e) 和 (n, d)。

加密：由 $c = m^e \bmod n$ 将明文 m 转变为密文 c（即：当 m^e 除以 n 所得的余数）。

注意：$m < n$ （如果需要，则分块）

解密：$m = c^d \bmod n$（即：c^d 除以 n 所得的余数）。

核心思想：$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

RSA公钥加密体制原理

由欧拉定理得出：

当 $\gcd(a, N) = 1$ 时， $a^{\phi(N)} \bmod N = 1$

在RSA中有：

1. $N = p \cdot q$
2. $\phi(N) = (p-1)(q-1)$
3. 选择整数 e 和 d ，d 为 e 关于模 $\phi(N)$ 的模反元素
4. $e \cdot d = 1 + k \cdot \phi(N)\,(k > 0, k \in Z)$

于是有： $C^d = (M^e)^d = M^{1+k\cdot\phi(N)} = M^1 \cdot (M^{\phi(N)})^k$

$$= M^1 \cdot (1)^k = M^1 = M \bmod N$$

RSA公钥加密体制原理

Bob选择 $p=5, q=7$ ，则 $n=35, z=24$ 。 $e=5$（所以 e, z互为质数） $d=29$ （所以 $ed-1$ 能完全被z整除 ）。

加密：

$\underline{letter}$	$\underline{m}$	$\underline{m^e}$	$\underline{c = m^e \bmod n}$
1	12	1524832	17

解密：

$\underline{c}$	$\underline{c^d}$	$\underline{m = c^d \bmod n}$	$\underline{letter}$
17	481968572106750915091411825223071697	12	1

感 谢 聆 听!

xionghu.uestc@gmail.com