

THE RSA ALGORITHM

- Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978.
- The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n .
- A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024} .

DESCRIPTION OF THE ALGORITHM

- RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n .
- That is, the block size must be less than or equal to $\log_2(n) + 1$; in practice, the block size is i bits, where $2^i n \leq 2^{i+1}$.
- Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C
- $C = M^e \bmod n$
- $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$
- Both sender and receiver must know the value of n .
- The sender knows the value of e , and only the receiver knows the value of d .
- Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$.

REQUIREMENTS

- For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.
- 1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
- 2. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.
- 3. It is infeasible to determine d given e and n .
- Need to find a relationship of the form $M^{ed} \bmod n = M$
- The preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function.
- for p, q prime, $\phi(pq) = (p - 1)(q - 1)$.
- The relationship between e and d can be expressed as $ed \bmod \phi(n) = 1$

THE RSA ALGORITHM

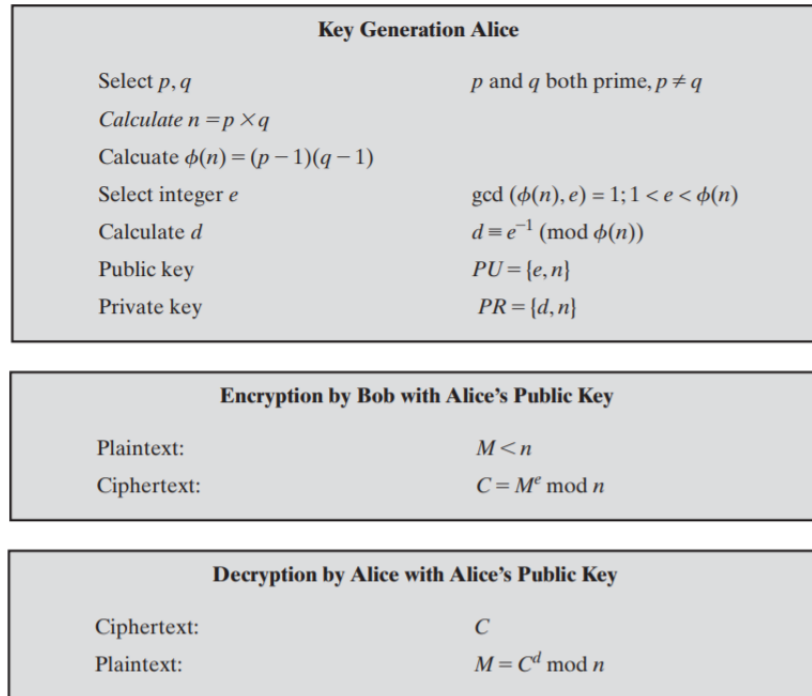


Figure 9.5 The RSA Algorithm

Reference : William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

