Public Key Cryptography

Part 2

RSA Algorithm

- Named after Ron Rivest, Adi Shamir, and Len Adleman who invented this algorithm at MIT in 1977.
- It is a Block Cipher.
- Plaintext and ciphertext are integers between 0 and (n – 1) for some n.

Some Relevant Facts about Numbers

- **Prime number p**:
  - p is an integer
  - $p \geq 2$
  - The only divisors of p are 1 and p
- Examples
  - $2, 5, 7, 11, 13, 17, 19$ are primes
  - $-3, 0, 1, 6$ are not primes
- **Prime decomposition** of a positive integer n:

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

- Example:
  - $200 = 2^3 \times 5^2$

Fundamental Theorem of Arithmetic

The prime decomposition of a positive integer is unique

Greatest Common Divisor

- The **Greatest Common Divisor** (GCD) or **Highest Common Factor** (HFC) of two positive integers $\boldsymbol{a}$ and $\boldsymbol{b}$, denoted $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b})$, is the largest positive integer that divides both $\boldsymbol{a}$ and $\boldsymbol{b}$.
- The above definition is extended to arbitrary integers.
- Examples:

$$\gcd(18, 30) = 6 \qquad \gcd(0, 20) = 20$$
$$\gcd(-21, 49) = 7$$

- Two integers a and b are said to be ***relatively prime*** if

$$\gcd(a, b) = 1$$

- Example:
  - Integers 15 and 28 are relatively prime.

RSA Algorithm

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

RSA Cryptosystem

- **Setup:**
  - $n = p.q$, with p and q primes
  - e relatively prime to $\phi(n) = (p-1)\,(q-1)$
  - d inverse of e in $Z_{\phi(n)}$
- **Keys:**
  - Public key: $K_E = (n, e)$
  - Private key: $K_D = (n, d)$
- **Encryption:**
  - Plaintext M in Z_n
  - $C = M^e \bmod n$
- **Decryption:**
  - $M = C^d \bmod n$

- Example
  - **Setup:**
    - $p = 7, \;\; q = 17$
    - $n = 7 \cdot 17 = 119$
    - $\phi(n) = (7-1)\cdot(17-1) = 6\cdot 16 = 96$
    - $e = 5$ [relatively prime to $\phi(n)$]
    - $d = 77$ [$77 \text{x} 5 \bmod \phi(n) = 1$]
  - **Keys:**
    - public key: (119, 5)
    - private key: (119, 77)
  - **Encryption:**
    - $M = 19$
    - $C = 19^5 \bmod 119 = 66$
  - **Decryption:**
    - $M = 66^{77} \bmod 119 = 19$

Online RSA Tool

https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo

Another Example

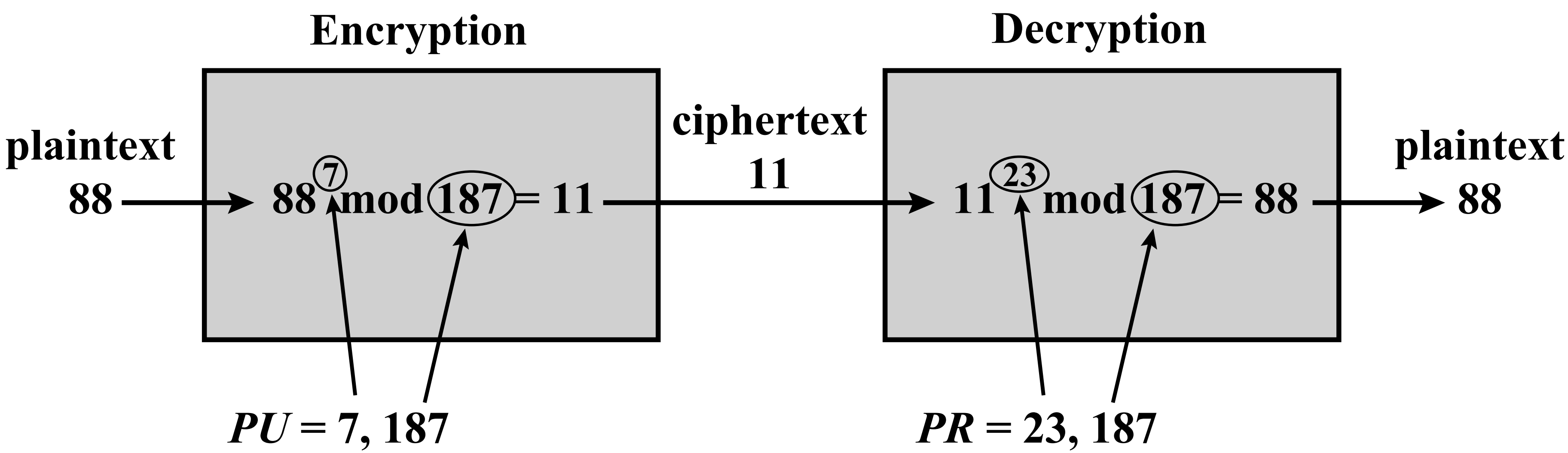

Figure 3.11 Example of RSA Algorithm

Complete RSA Example

- Setup:
  - $p = 5, q = 11$
  - $n = 5 \cdot 11 = 55$
  - $\phi(n) = (5-1)\cdot(11-1) = 4\cdot 10 = 40$
  - $e = 3$
  - $d = 27$ $[e \cdot d = 3 \cdot 27 = 81 = 2 \cdot 40 + 1]$
- **Encryption**
  - $C = M^3 \bmod 55$
- **Decryption**
  - $M = C^{27} \bmod 55$

M	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
C	1	8	27	9	15	51	13	17	14	10	11	23	52	49	20	26	18	2
M	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
C	39	25	21	33	12	19	5	31	48	7	24	50	36	43	22	34	30	16
M	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
C	53	37	29	35	6	3	32	44	45	41	38	42	4	40	46	28	47	54

References

- Book: Cryptography and Network Security – Principles and practice, 7th Edition.
  - Section 9.1: Principles of Public-key Cryptosystems
  - Section 9.2: The RSA Algorithm