

4.6 Cryptography

In this section, we explore some number theoretical methods to encode/decode a message.

Shift Encryption/Decryption ((Ceasar Cipher/Decipher):

Fix a number p (e.g. in Ceasar cipher we choose $p=3$).

Consider $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$ and suppose $\mathbb{Z}_{26}$ represents the alphabet $\{a, b, \dots, z\}$. The function $\begin{cases} E: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26} \\ E(x) = x + p \end{cases}$

is called the shift encryption function. e.g. when $p=3$:

$E(0)=3$	$a \rightarrow d$
$E(1)=4$	$b \rightarrow e$
$\vdots$	$\vdots$
$E(25)=2$	$z \rightarrow c$

The function $\begin{cases} D: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26} \\ D(x) = x - p \end{cases}$ is the

decryption function for E because:

$$\forall M \in \mathbb{Z}_{26} : D(E(M)) = D(M+p) = M+p-p = M$$

Affine Encryption/Decryption:

Fix a number p and a number a so that $\gcd(a, 26) = 1$.

The function $\begin{cases} E: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26} \\ E(x) = ax + p \end{cases}$ is called an affine encryption.

note that $\gcd(a, 26) = 1$

(note that E is one-to-one because: $E(x) \equiv E(y) \implies x \equiv y$ and therefore E is an encryption function)

The function $\begin{cases} D: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26} \\ D(x) = \bar{a}(x-p) \end{cases}$ [where $\bar{a}$ is the inverse of a modulo 26 (note that $\bar{a}$ exists because $\gcd(a, 26) = 1$)]

is the decryption function for E because: $\forall M \in \mathbb{Z}_{26}$:

$$D(E(M)) = D(aM+p) = \bar{a}(aM+p-p) = \bar{a}aM = 1M = M$$

$$D(E(M)) = D(aM + p) = a(aM + p - p) = \bar{a}aM = 1 \cdot M = M$$

4.6. CRYPTOGRAPHY

CHAPTER 4.

RSA Encryption: We have two "public" keys: n and e .

where $n = p \cdot q$, p and q are two "large" primes and

e is an integer such that $\gcd(e, (p-1)(q-1)) = 1$.

(p and q are "private" (secret) keys).

Given a plaintext $M \in \mathbb{Z}$:
$$\begin{cases} E: \mathbb{Z} \rightarrow \mathbb{Z} \\ E(M) = M^e \bmod n. \end{cases}$$

is called the RSA encryption function.

Example 4.6.1. Encrypt the integer 3 using the RSA encryption with $(n, e) = (33, 13)$.

$$n = 33 = \underset{p}{3} \times \underset{q}{11} = pq \quad \text{where } p=3, q=11.$$

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 2 \times 10) = \gcd(13, 20) = 1$$

$$M=3 \quad E(M) = M^e \bmod n = 3^{13} \bmod 33$$

$$13 = (1101)_2$$

$$13 = 8 + 4 + 1$$

$$\begin{aligned} 3^1 \bmod 33 &= 3 \\ 3^2 &\equiv 9 \pmod{33} \\ 3^4 &\equiv 15 \pmod{33} \\ 3^8 &\equiv 27 \pmod{33} \end{aligned}$$

(Note: A bracket indicates that the powers 1, 2, 4, 8 are summed to get 13, with the instruction "raise both sides to power 2".)

$$= 27$$

$$\begin{array}{r} -90 + \\ \underline{-99} \\ 9 \end{array}$$

$$\begin{array}{r} 27 \\ -33 \\ \hline -6 \end{array}$$

$$198 = 6 \times 33$$

$$\begin{array}{r} 81 \\ -66 \\ \hline 15 \end{array}$$

$$\begin{array}{r} 15^2 = 225 \\ -198 \\ \hline 27 \end{array}$$

$$\begin{aligned} \therefore 3^{13} &= 3^8 \cdot 3^4 \cdot 3^1 = 27 \cdot 15 \cdot 3 = (-6)(15)(3) = -90 \times 3 \\ &= 9 \times 3 = 27 \end{aligned}$$

$$\therefore 3^{15} = 3^8 \cdot 3^7 \cdot 3^0 \equiv 27 \cdot 15 \cdot 3 \equiv (-6)(15)(3) \equiv \begin{matrix} -90 \times 3 \\ 9 \times 3 \equiv 27 \\ (\text{mod } 33) \end{matrix}$$

4.6. CRYPTOGRAPHY

CHAPTER 4.

RSA Decryption: Since $\gcd(e, (p-1)(q-1)) = 1$, we know that e has a multiplicative inverse modulo $(p-1)(q-1)$:

$$\exists \bar{e} \in \mathbb{Z} : \bar{e} e \equiv 1 \pmod{(p-1)(q-1)}$$

(we usually use d instead of $\bar{e}$: $d = \bar{e}$)

$$\exists d \in \mathbb{Z} : de \equiv 1 \pmod{(p-1)(q-1)}$$

The number d is the "secret" key for decryption:

Claim: The function $\begin{cases} D: \mathbb{Z} \rightarrow \mathbb{Z} \\ D(x) = x^d \pmod{n} \end{cases}$ is

the decryption function for the RSA encryption function E .

Proof. We need to prove: $\forall M \in \mathbb{Z} : D(E(M)) = M$.

Since $de \equiv 1 \pmod{(p-1)(q-1)} \exists k \in \mathbb{Z} : de = k(p-1)(q-1) + 1$

Consider two cases. Case 1 M is a multiple of p or q
(Exercise: show $D(E(M)) = M$)

Case 2 M is not a multiple of p and not a multiple of q .

By Fermat's little Theorem: $M^{p-1} \equiv 1 \pmod{p}$, $M^{q-1} \equiv 1 \pmod{q}$

Then $(M^{p-1})^{k(q-1)} \equiv 1 \pmod{p}$: $M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$

$\therefore M^{k(p-1)(q-1)} \cdot M^1 \equiv 1 \cdot M \pmod{p}$: $M^{k(p-1)(q-1)+1} \equiv M \pmod{p}$

$\therefore M^{de} \equiv M \pmod{p}$: $p \mid M^{de} - M$. Similarly: $q \mid M^{de} - M$.

Since p and q are two primes, we get $pq \mid M^{de} - M$. Since $n = pq$

$\therefore n \mid M^{de} - M$: $M^{de} \equiv M \pmod{n}$: $(M^e)^d \pmod{n} = M$

Example 4.6.2. Decrypt the integer 27 using the RSA encryption with $(n, e) = (33, 13)$.

(from the previous example we expect the answer to be 3).

$$n = 33 = 3 \times 11 = pq, \quad p = 3, \quad q = 11.$$

$$\text{Let } d = \text{inverse of } e \text{ modulo } (p-1)(q-1) \\ = \text{inverse of } 13 \text{ modulo } 20.$$

$$13 \cdot \overset{d}{\boxed{}} \equiv 1 \pmod{20}$$

To find d , either guess or use Euclidean algorithm:

$$20 = 13 \cdot \boxed{1} + \boxed{7} \rightarrow \boxed{7} = \boxed{1} \cdot 20 + \boxed{-1} \cdot 13$$

$$13 = 7 \cdot \boxed{1} + \boxed{6} \rightarrow \boxed{6} = \boxed{1} \cdot 13 + \boxed{-1} \cdot 7$$

$$7 = 6 \cdot \boxed{1} + \boxed{1} \rightarrow \boxed{1} = \boxed{1} \cdot 7 + \boxed{-1} \cdot 6$$

$$= \boxed{1} \cdot 7 + \boxed{-1} (\boxed{1} \cdot 13 + \boxed{-1} \cdot 7)$$

$$= \boxed{2} \cdot 7 + \boxed{-1} \cdot 13$$

$$= \boxed{2} (\boxed{1} \cdot 20 + \boxed{-1} \cdot 13) + \boxed{-1} \cdot 13$$

$$= \boxed{2} \cdot 20 + \boxed{-3} \cdot 13$$

$\therefore$ note that $-3 \equiv 17 \pmod{20}$

$\therefore d = 17$ is the inverse of 13 modulo 20.

$$D(27) = 27^{17} \pmod{33} = 3$$

$$17 = 16 + 1 \quad 27^1 \equiv 27 \pmod{33} \quad 79 \\ 27^2 \equiv (-6)^2 \equiv 36 \equiv 3$$

$$27^4 \equiv (27^2)^2 \equiv (3)^2 \equiv 9$$

$$27^8 \equiv (27^4)^2 \equiv (9)^2 \equiv 81 \equiv 15$$

$$27^{16} \equiv (27^8)^2 \equiv (15)^2 \equiv 225 \equiv 225 - 198 \equiv 27$$