Public Key Cryptography

In this section we briefly look at the RSA cryptosystem.

First, we look at an example and then we prove why it works.

Example: Suppose we need to send the following message

PUBLIC KEY CRYPTOGRAPHY

Step 1: Translate each letter to its numerical equivalent (such as ASCII). For the sake of simplicity we use the following table.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical Equivalent	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 8.9 *Two-digit numerical equivalents of letters.*

Step 2: We group the translated number to blocks of 4 digits as follows.

1520	0111	0802	1004
2402	1724	1519	1406
1700	1507	2423,	

Note that $x = 23$ is inserted at the end to make it a block of 4 digits.

Step 3: Choose two very large primes p and q. Usually, p and q contain thousand of digits, but for illustrative purpose we choose $p = 43$ and $q = 59$.

Step 4: Let $n = pq = 43 \cdot 59 = 2537$.

n is called the modulus.

Choose e such that $\gcd(e, \varphi(n)) = 1$.

e is called the exponent.

Let's choose $e = 13$.

It's easy to see that

$$\gcd(e, \varphi(n)) = \gcd(13, \underbrace{42 \cdot 58}_{=2436})$$
$$= 1$$

Step 5: We encrypt each 4-digit block P into a cyphertext block C using the formula

$$C \equiv P^e \pmod{n}$$

i.e., $$C \equiv P^{13} \pmod{2537}$$

For instance, the first block 1520 is encrypted to 95:

$$C \equiv 1520^{13} \pmod{2537}$$
$$\equiv 95 \pmod{2537}$$

Note that 95 can be obtained by using a method such as "fast modular exponentiation" explained in section 4.1.

When all blocks are encrypted, we get the following cyphertext message.

0095	1648	1410	1299
0811	2333	2132	0370
1185	1957	1084.	

Step 6: To decrypt this message, we have to choose a decryption key d. We find d as an inverse of e modulo $\varphi(n)$. That is, d is found such that

$$ed \equiv 1 \pmod{\varphi(n)}.$$

i.e., $$13d \equiv 1 \pmod{2436}$$

In this case, using the Euclidean algorithm, we find

$$d = 937.$$

Finally, we decrypt the message using the formula

$$P \equiv C^{937} \pmod{2537}, \quad 0 \leq P < 2537$$

For instance, for $C = 95$, we get

$$95^{937} \equiv 1520 \pmod{2537}$$

Now, let's explain why this works.

Let p and q be primes and $n = pq$.
Also, let e be chosen such that $\gcd(e, \varphi(n)) = 1$.

Let d be an inverse of e modulo $\varphi(n)$, i.e., let

$$ed \equiv 1 \pmod{\varphi(n)}. \quad -①$$

Such d exists because $\gcd(e, \varphi(n)) = 1$.

Let P be a plaintext. We encrypt P to get C using the congruence

$$E(P) = C \equiv P^e \pmod{n}, \quad 0 \le C < n \quad -②$$

To get P from C, i.e., to decrypt C to get P, we use the congruence

$$D(C) = C^d \equiv \pmod{n}.$$

Let's prove that $D(C) \equiv P \pmod{n}$

We've

$$\begin{aligned} D(C) &= C^d \\ &\equiv (P^e)^d \pmod{n} \quad (\text{by } ②) \\ &\equiv P^{ed} \pmod{n} \end{aligned}$$

$$\equiv P^{1+k\varphi(n)} \pmod{n} \quad (\because \text{ by } ①,\ ed \equiv 1 \pmod{\varphi(n)}$$

so, $ed - 1 = k\varphi(n)$)

$$\equiv P \cdot \left(P^{\varphi(n)}\right)^k \pmod{n}$$

Now, if $\gcd(P, n) = 1$, then by Euler's theorem, $P^{\varphi(n)} \equiv 1 \pmod{n}$ and therefore, we have

$$\equiv P\ 1^k \pmod{n}$$

$$\equiv P \pmod{n}$$

as desired. If, in the very rare case, $\gcd(P, n) > 1$, then we can still show that $D(C) = P$ by using the Chinese remainder theorem as follows.

If $p \nmid P$, then

$$D(C) \equiv P^{1+k\varphi(n)}$$

$$\equiv P \cdot P^{k(p-1)(q-1)} \quad (\because \varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1))$$

$$\equiv P \left(P^{p-1}\right)^{k(q-1)}$$

$$\equiv P 1^{k(q-1)} \pmod{p} \quad (\because \text{ by Fermat's little theorem, } P^{p-1} \equiv 1 \pmod{n})$$

$$\equiv P$$

If $p \mid P$, then $P \equiv 0 \pmod{p}$, so

$$C = P^e \equiv 0 \pmod{p}$$

and hence

$$\begin{aligned} D(C) &\equiv C^d \\ &\equiv (P^e)^d \\ &\equiv 0^d \\ &\equiv 0 \\ &\equiv P \pmod{p} \end{aligned}$$

Hence, in any case, $D(C) \equiv P \pmod{p}$.

Similarly,

$$D(C) \equiv P \pmod{q}$$

Using the Chinese remainder theorem, we get

$$D(C) \equiv P \pmod{pq}$$

i.e.,

$$D(C) \equiv P \pmod{n}$$

as desired.

Note that, the Chinese remainder theorem argument is valid for the case $\gcd(P, n) = 1$ too!