section 4.6

RSA

$n = p \cdot q$

Encryption

$c = m^e \bmod n$

Key(n, e) ← both n and e are given p.q also given

m is the block of the original message.
(the integer representation of it)

$\gcd(e,(p-1)(q-1)) = 1$ ← You'll utilize this fact for decryption

encrypted message(integer)

Blocks of M:

Divide the original message into equally sized blocks of 2N digits, where 2N is the largest even number such that the number 2525....25 with 2N digits doesn't exceed n.

This passage tells you what the block size is.

ex: if $n = 2537$

$2525 < 2537$

largest grouping of 25's that doesn't exceed n because 2525 is four digits, the block size is four.

ex: if $n = 713345$

$252525 < 713345$

↖ because it's six digits, block size is six

$n = 113345$

$2525 < 113345$

block size is 4

For RSA,
A to J is two digits, padded with Ø on the left.

e.g. A is 00
B is 01
etc

pad last block with x's if it doesn't meet the block size.

ex:

Encrypt the message STOP using RSA with key(2537, 13).
Note that $2537 = 43 \cdot 59$. $p = 43$, $q = 59$ and they're primes

$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$

Solution:

Block size: $2525 < 2537$, so each block is size 4.

convert letters to numbers: STOP
18, 19, 14, 15

$m_1 = 1819$
$m_2 = 1415$

$c_1 = m_1^e \bmod n$ $\quad c_2 = m_2^e \bmod n$

STOPS
$m_1 = 1819$
$m_2 = 1415$
$m_3 = 18\textcircled{23} \leftarrow x$

$c_1 = 1819^{13} \bmod 2537$ $\longleftrightarrow$ $c_2 = 1415^{13} \bmod 2537$

use modular exponentiation

$c_2 = 2182$

$(13)_{10} = (1101)_2$

$\checkmark\ 1819^1 \bmod 2537 = 1819$

$1814^2 \bmod 2537 = 513$

$\checkmark\ 1819^4 \bmod 2537 = 513^2 \bmod 2537 = 1858$

$\checkmark\ 1819^8 \bmod 2537 = 1858^2 \bmod 2537 = 1844$

$(1819 \cdot 1858 \cdot 1844) \bmod 2537 = 2081$

$$\boxed{2081 \quad 2182}$$