Lecture 7.2

Last time:

- Congruences $x^k \equiv a \pmod{n}$ can be solved if $\gcd(a,n) = 1$, $\gcd(k, \phi(n)) = 1$ and one solution satisfies

$$x \equiv a^u \pmod{n}$$

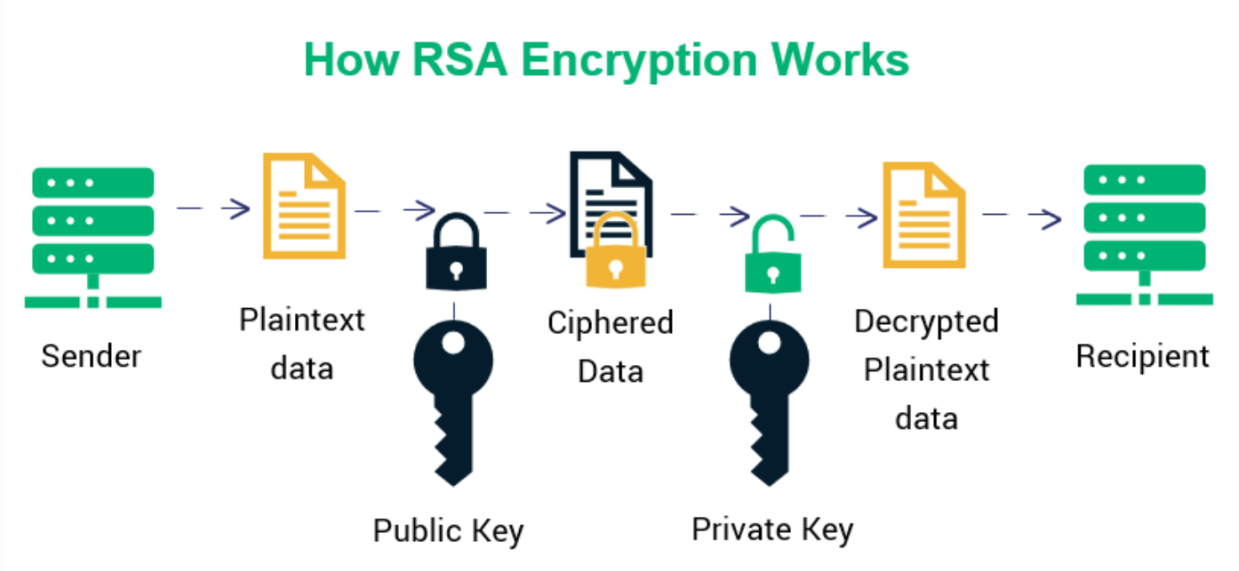
where $ku + \phi(n)v = 1$.

- $a^u \pmod{n}$ can be evaluate with successive squaring.

Lecture 7.3

RSA Cryptography

Public key cryptography is any scheme for sending an encoded message in which the encoding operation (the public key) may be unsecure, but the decoding operation (the private key) is concealed.



This diagram lays out the steps in any public key cryptosystem. We will learn about a specific method for producing a public and private key and how to use them to send a message securely. This is due to Rivest, Shamir and Adleman.

The first step is to encode a message as a "word", or a number w

whose digits represent the letters of

the message.

For example, we could assign the numbers

1 - 26 to A - Z and create W

out of words and phrases:

HELLO ⇝ 08 05 12 12 15

NUMBER ⇝ 14 21 13 02 05 18

THEORY ⇝ 20 08 05 15 18 25

Using the computer alphabet ASCII, we

will instead start at 65 (or 97):

ASCII Table

<linuxhint/>

Code Char		Code Char	Code Char	Code Char
0	NUL (null)	32 SPACE	64 @	96 `
1	SOH (start of heading)	33 !	65 A	97 a
2	STX (start of text)	34 "	66 B	98 b
3	ETX (end of text)	35 #	67 C	99 c
4	EOT (end of transmission)	36 $	68 D	100 d
5	ENQ (enquiry)	37 %	69 E	101 e
6	ACK (acknowledge)	38 &	70 F	102 f
7	BEL (bell)	39 '	71 G	103 g
8	BS (backspace)	40 (	72 H	104 h
9	TAB (horizontal tab)	41)	73 I	105 i
10	LF (NL line feed, new line)	42 *	74 J	106 j
11	VT (vertical tab)	43 +	75 K	107 k
12	FF (NP form feed, new page)	44 ,	76 L	108 l
13	CR (carriage return)	45 -	77 M	109 m
14	SO (shift out)	46 .	78 N	110 n
15	SI (shift in)	47 /	79 O	111 o
16	DLE (data link escape)	48 0	80 P	112 p
17	DC1 (device control 1)	49 1	81 Q	113 q
18	DC2 (device control 2)	50 2	82 R	114 r
19	DC3 (device control 3)	51 3	83 S	115 s
20	DC4 (device control 4)	52 4	84 T	116 t
21	NAK (negative acknowledge)	53 5	85 U	117 u
22	SYN (synchronous idle)	54 6	86 V	118 v
23	ETB (end of trans. block)	55 7	87 W	119 w
24	CAN (cancel)	56 8	88 X	120 x
25	EM (end of medium)	57 9	89 Y	121 y
26	SUB (substitute)	58 :	90 Z	122 z
27	ESC (escape)	59 ;	91 [	123 {
28	FS (file separator)	60 <	92 \	124 |
29	GS (group separator)	61 =	93]	125 }
30	RS (record separator)	62 >	94 ^	126 ~
31	US (unit separator)	63 ?	95 _	127 DEL

HELLO ⇝ 72697767679

NUMBER $\rightsquigarrow$ 78857766982

THEORY $\rightsquigarrow$ 847269798289

The next step is to encrypt our word.

Theorem Let p, q be distinct primes and set $N = pq$. Then for any $W < N$ with $\gcd(W, N) = 1$ and any $k \in \mathbb{N}$,

(1) $W^{1+k(p-1)(q-1)} \equiv W \pmod{N}$.

(2) For any $E \in \mathbb{N}$ with $\gcd(E, (p-1)(q-1)) = 1$,

there exists some $D \in \mathbb{N}$ such that

$$W^{ED} \equiv W \pmod{N}.$$

Pf: (1) Notice that

$$\phi(N) = \phi(pq) = (p-1)(q-1)$$

so by Euler's theorem,

$$W^{1+k(p-1)(q-1)} \equiv W \cdot (W^{\phi(N)})^k$$

$$\equiv W \cdot 1^k \equiv W \pmod{N}.$$

(2) Since $\gcd(E, (p-1)(q-1)) = 1$, the linear equation

$$Ex + (p-1)(q-1)y = 1$$

has a solution, say with $x = D \in \mathbb{N}$

and $y = -k$. Then

$$W^{ED} = W^{1+k(p-1)(q-1)} \equiv W \pmod{N}$$

by (1). □

RSA Algorithm

Step 1: Encode a message as $W \in \mathbb{N}$.

Step 2: Choose p, q prime so that $W < pq$.

Set $N = pq$.

Step 3: Choose an encryption key E and a decryption key D satisfying $\gcd(E, \phi(N)) = 1$, $ED \equiv 1 \pmod{\phi(N)}$.

Step 4: To encrypt, compute W^E.

Step 5: To decrypt, compute $(W^E)^D$. We know $W^{ED} \equiv W \pmod{N}$.

How secure is this?

As long as the factors of N are concealed, it is extremely difficult to "break" the cryptosystem by finding

to break the

D satisfying $ED \equiv 1 \pmod{\phi(N)}$.

Currently, the largest $N = pq$ to have been factored by computers (with state-of-the-art algorithms) has 250 digits.

So as long as p and q are large enough, N will be secure.

(Quantum computing may provide a major leap in decryption power though...)

Ex To practice, let's scramble single

letter : Q $\rightsquigarrow$ $W = 17$.

Choose : $N = 21 = 3 \cdot 7$

$\phi(N) = 2 \cdot 6 = 12$

$E = 5$ $\quad \gcd(5, 12) = 1$ ✓

$D = 5$ $\quad 5 \cdot 5 + 12(-2) = 1$ ✓

Encrypt : $W^E = 17^5 = 17^4 \cdot 17$

k	2^k	$17^{2^k} \pmod{21}$
1	2	$17^2 \equiv (-4)^2 \equiv 16$
2	4	$16^2 \equiv (-5)^2 \equiv 25 \equiv 4$

$\rightsquigarrow$ $17^5 \equiv 4 \cdot 17 \equiv 4 \cdot (-4)$

$\equiv -16 \equiv 5 \pmod{21}$.

Decrypt: $(W^E)^D = 5^5 = 5^4 \cdot 5$

k	2^k	$5^{2^k} \pmod{21}$
1	2	$5^2 = 25 \equiv 4$
2	4	$4^2 = 16$

$\rightsquigarrow$ $5^5 \equiv 16 \cdot 5 \equiv -5 \cdot 5$

$\equiv -25 \equiv -4 \equiv \underset{\sim}{17} \pmod{21}$.

$\underset{\sim}{W}$ ✓

Exercise 1: Suppose I send you the

encrypted message $W^E = 265$ the modulo

encrypted message $W = 203$, the modulus $N = 7519$ and the private key $D = 5$.

(a) What message did I send you? Remember to translate using the ASCII table.

(b) Can you break the code directly if I tell you one of the prime factors of N has two digits?

Exercise 2: For $N = 1537$,

(a) Check that $E = 47$ and $D = 31$ are a valid pair of keys.

(b) Describe how to send the word

$W = 131$ securely.

(c) What's the longest English word you can send (using ASCII)?

Next time: quadratic residues.