CS285 PROJECT

made by: Nora Alrubayan 220410543
Shog Alhargan 220410521

SECTION: 876

RSA ALGORITHM

History

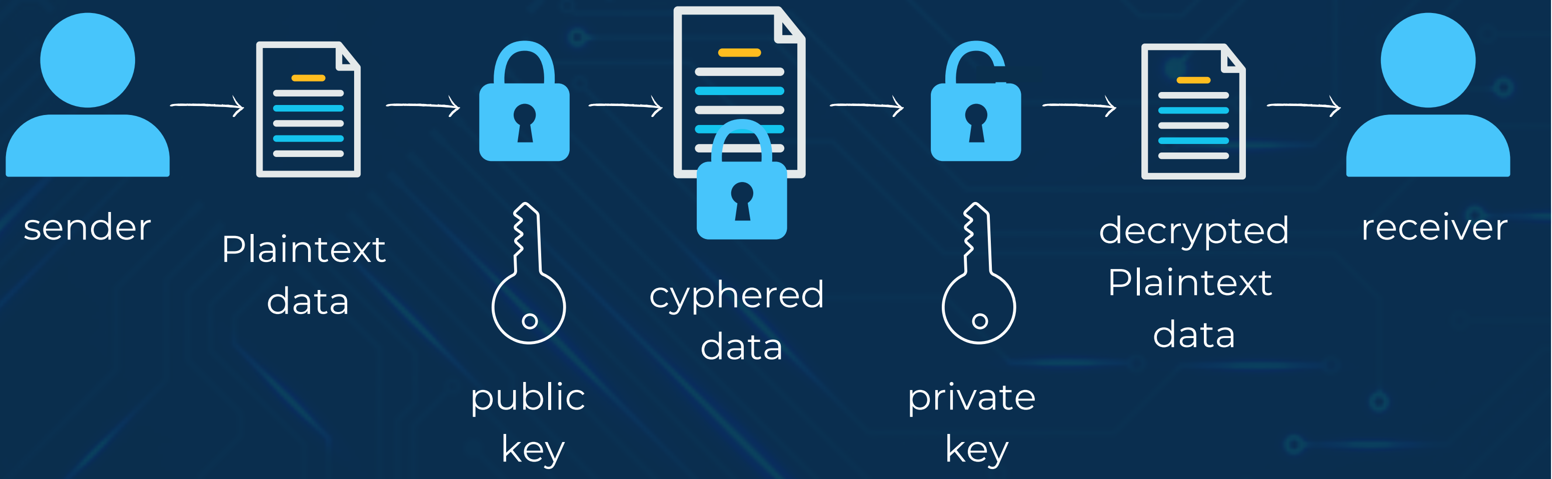
RSA algorithm was invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman and was named after them. It was founded because they wanted to pursue commercial applications.

Description

RSA algorithm is a way to send and receive encrypted messages between each other, only for them to be decrypted by using a public and a private key.

1. The sender first encrypts the message using the receiver's private key.
   Now we have the cyphered text.
2. The cyphered text is now transmitted to the receiver (without any other key).
   after receiving the cyphered text
3. The receiver uses his private key to decrypt the cyphered text.

Visualization



KEYS GENERATION

1. *pick two small prime numbers (P,Q):*
P = 5 , Q = 7

2. *find Z, using Z = (P-1)*(Q-1):*
Z = (5-1)(7-1)*
Z = (4)(6) = 24 --> (secret)*

3. *find N, using N = P*Q:*
N = (5)(7) = 35*

4. *pick a public-key exponent E:*
the rule: 1 < E < Z
E = 11

5. *private exponent D, D = ((Z*i)+1)/E*
*D=((24*1)+1)/11= 2.27*
*D=((24*2)+1)/11=4.45*
*D=((24*3)+1)/11=6.63*
*D=((24*4)+1)/11=8.81*
*D=((24*5)+1)/11= 11 We will stop here*

6. *set of keys:*
a. public key {E,N} = {11,35} -->sender
b. private key {D,N} = {11,35} -->receiver

ENCRYPTION & DECRYPTION

space	0	a	1	b	2
c	4	d	4	e	5
f	6	g	7	h	8
i	9	j	10	k	11
l	12	m	13	n	14
o	15	p	16	q	17
r	18	s	19	t	20
u	21	v	22	w	23
x	24	y	25	z	26

- *The message before encryption:*

> *"Everyone should learn how to code, it teaches you how to think"*
>
> *-Steve Jobs*

ENCRYPTION

using the public key = {E,N} = {11,35}
and the formula: L^E(mod N)

E=5 --> 5^11 mod(35) = 10=J	**V=22** --> 22^11 mod(35) = 8=H	**R=18** --> 18^11 mod(35) = 2=B
Y=25 --> 25^11 mod(35) = 30=??	**O=15** --> 15^11 mod(35) = 15=O	**N=14** --> 14^11 mod(35) = 14=N
S=19 --> 19^11 mod(35) = 24=X	**H=8** --> 8^11 mod(35) = 22=V	**U=21** --> 5^11 mod(35) = 21=U
L=12 --> 12^11 mod(35) = 3=C	**D=4**--> 4^11 mod(35) = 9=I	**A=1**--> 1^11 mod(35) = 1=A
W=23 --> 23^11 mod(35) = 32=??	**T=20** --> 20^11 mod(35) = 20=T	**C=3** --> 3^11 mod(35) = 12=L
I=9 --> 9^11 mod(35) = 4=D	**K=11** --> 11^11 mod(35) = 16=P	

For y and w, we weren't able to decode them. Because after using the formula, their numbers exceeded 26.

Y=25 --> 25^11 mod(35) = 30=??

W=23 --> 23^11 mod(35) = 32=??

ENCRYPTION

using the public key = {E,N} = {11,35}
and the formula: L^E(mod N)

E	V	E	R	Y	O	N	E
5	22	5	18	25	15	14	5
J	H	J	B	?	O	N	J

S	H	O	U	L	D
19	8	15	21	12	4
X	V	O	U	C	I

L	E	A	R	N
12	5	1	18	14
C	J	A	B	N

H	O	W
8	15	23
V	O	?

T	O
20	15
T	O

C	O	D	E
3	15	4	5
L	O	I	J

I	T
9	20
D	T

T	E	A	C	H	E	S
20	5	1	3	8	5	19
T	J	A	L	V	J	X

Y	O	U
25	15	21
?	O	U

H	O	W
8	15	23
V	O	?

T	O
20	15
T	O

T	H	I	N	K
20	8	9	14	11
T	V	D	N	P

- *The message after encryption: "JHJB?ONJ XVOUCI CJABN VO? TO LOIJ DT TJALVJX ?OU VO? TO TVDNP”*

DECRYPTION

using the public key = {E,N} = {11,35}
and the formula: L^D(mod N)

J=10 --> 10^11 mod(35) = 5=3	**H=8** --> 8^11 mod(35) = 22=V	**B=2** --> 2^11 mod(35) = 18=R
??	**O=15** --> 15^11 mod(35) = 15=O	**N=14** --> 14^11 mod(35) = 14=N
X=24 --> 24^11 mod(35) = 19=S	**V=22** --> 22^11 mod(35) = 8=H	**U=21** --> 5^11 mod(35) = 21=U
C=3 --> 3^11 mod(35) = 12=L	**I=9**--> 9^11 mod(35) = 4=D	**A=1**--> 1^11 mod(35) = 1=A
??	**T=20** --> 20^11 mod(35) = 20=T	**L=12** --> 12^11 mod(35) = 4=C
D=4 --> 4^11 mod(35) = 9=I	**P=16** --> 16^11 mod(35) = 11=K	

DECRYPTION

using the public key = {E,N} = {11,35}
and the formula: L^D(mod N)

J	H	J	B		O	N	J
10	8	10	2		15	14	10
E	V	E	R	?	O	N	E

X	V	O	U	C	I
24	22	15	21	3	9
S	H	O	U	L	D

C	J	A	B	N
3	10	1	2	14
L	E	A	R	N

V	O	
22	15	
H	O	?

T	O
20	15
T	O

L	O	I	J
12	15	9	10
C	O	D	E

D	T
4	20
I	T

T	J	A	L	V	J	X
20	10	1	12	22	10	24
T	E	A	C	H	E	S

	O	U
	15	21
?	O	U

V	O	
22	15	
H	O	?

T	O
20	15
T	O

T	V	D	N	P
20	22	4	14	16
T	H	I	N	K

- *The message after decryption:*
  "Ever?one should learn ho? to code it
  teaches ?ou ho? to think"

References:

- https://youtu.be/vf1z7GIG6Qo
- https://www.britannica.com/topic/RSA-encryption
- https://www.tausquared.net/pages/ctf/rsa.html