Information Security Lab End Term Project

Encryption using RSA algorithm and Keyword Cipher

Submitted by:
Divya Shikhar Chauhan 9919103021
Shubh Gupta 9919103022

Submitted to:
Himanshu Agrawal
Department of CSE & IT, JIIT-128

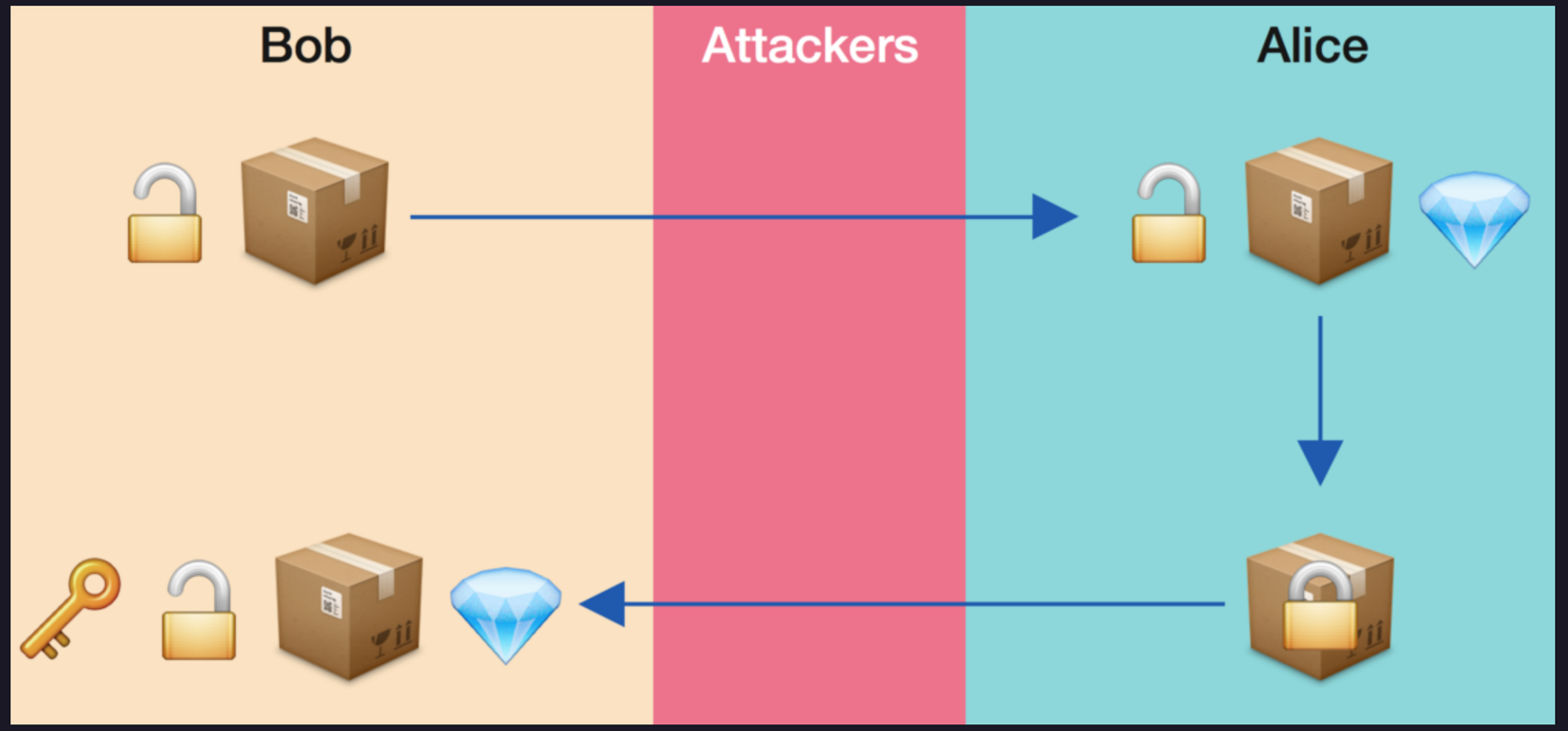
Communication is central in how we live.
Encryption ensures that your
communication is safe.

Let's see what RSA algorithm and Keyword cipher have for us then.

INTRODUCTION

The Rivest-Shamir-Adleman (RSA) encryption algorithm is an asymmetric encryption algorithm that is widely used in many products and services. Asymmetric encryption uses a key pair that is mathematically linked to encrypt and decrypt data. A private and public key are created, with the public key being accessible to anyone and the private key being a secret known only by the key pair creator. With RSA, either the private or public key can encrypt the data, while the other key decrypts it. This is one of the reasons RSA is the most used asymmetric encryption algorithm.

ASYMMETRIC KEY ENCRYPTION



HOW RSA ENCRYPTION WORKS?

RECEIVER

N,e

c= 89^e mod N

c= 1394

SENDER

msg= " H I "

8 9

1394

dcr = c^d mod N

dcr = 8 9

msg= " H I "

WHAT IS N, E, D?

- Think of number N, such that N= p*q, where p & q are very large prime numbers.
- Now think of e, such that 1 < e < (p-1)(q-1) and e and (p-1)(q-1) are co-prime.
- Your public key is ready! i.e. N and e.
- Sender encodes the data using c = (ASCII value)^e mod N.
- Now d should be such that it satisfies "ed mod (p-1)(q-1) = 1".
- Finalllyy, for decryption use c^d mod N and you got the ASCII codes.

KEYWORD CIPHER

A keyword cipher is a form of monoalphabetic substitution. A keyword is used as the key, and it determines the letter matchings of the cipher alphabet to the plain alphabet. Repeats of letters in the word are removed, then the cipher alphabet is generated with the keyword matching to A, B, C, etc.

In this case we have taken key as "Secret"

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
S	E	C	R	T	A	B	D	F	G	H	I	J	K	L	M	N	O	P	Q	U	V	W	X	Y	Z

Eg:

Plaintext = PREPARE FOR WAR

Ciphertext = MOTMSOT ALO WSO

P	R	E	P	A	R	E		F	O	R		W	A	R
M	O	T	M	S	O	T		A	L	O		W	S	O

RSA ENCRYPTION OF KEY "SECRET"

Keyword in ASCII form:

S	e	c	r	e	t
83	101	99	114	101	116

Eg:
Let us consider the first character in the keyword i.e "S", which corresponds to ASCII value 83.

P = 13 , Q = 11
N = P x Q = 143
Phi = (P-1) x (Q-1) = 120
e = 7
d = 103

C = (83 ^ e) % N
= (83 ^ 7) % 143
= 8

M = (C ^ d) % N
= (8 ^ 103) % 143
= 83

```
Plaintext : Prepare For War. Approaching from North-West.

Original Key:   Secret

Ciphered Text : MOTMSOT ALO WSO. SMMOLSCDFKB AOLJ KLOQD-WTPQ.

**********
RSA Values:

p = 13
q = 11
n = pq = 143
phi = 120
e = 7
d = 103
**********

Encrypted Key:   8 62 44 49 62 129
             :   >,1>ü

Decrypted Key:   83 101 99 114 101 116
             :   Secret

Deciphered Text: PREPARE FOR WAR. APPROACHING FROM NORTH-WEST.
```

AS YOU CAN SEE!

Encrypted text by RSA-

H[;!DbC-'n

On Decrypting-

Thank You!