Cairo University
Faculty of Engineering

Department of Computer Engineering

CMP3050– Spring 2023

Cryptography

About: RSA

Submitted by

Name	Sec	BN
Eslam Ashraf Ibrahim	1	13

What is the RSA algorithm (Rivest-Shamir-Adleman)?

The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

How does the RSA algorithm work?

Alice generates her RSA keys by selecting two primes: p=11 and q=13. The modulus is n=p*q=143. The totient is n ϕ(n)=(p−1)x(q−1)=120. She chooses 7 for her RSA public key e and calculates her RSA private key using the Extended Euclidean algorithm, which gives her 103.

Bob wants to send Alice an encrypted message, M, so he obtains her RSA public key (n, e) which, in this example, is (143, 7). His plaintext message is just the number 9 and is encrypted into ciphertext, C, as follows:

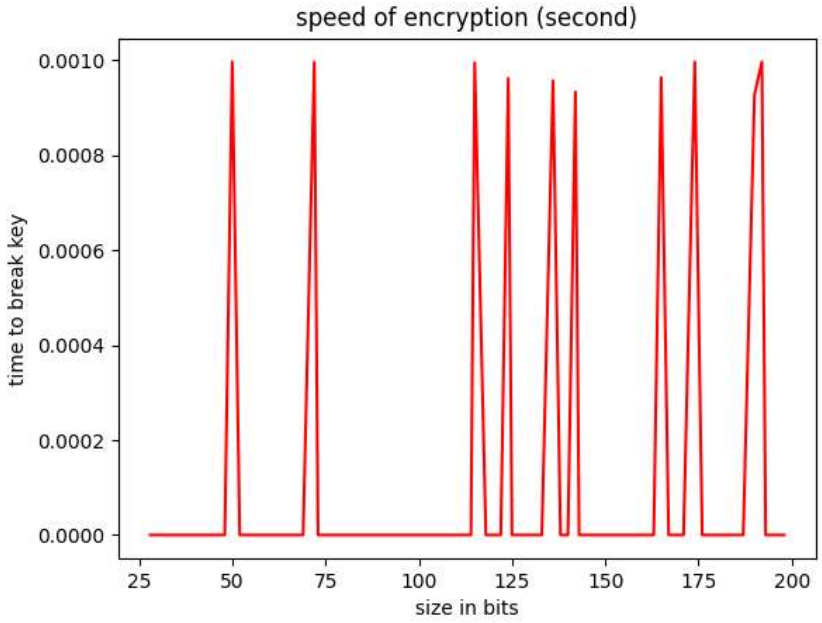
M^e mod n = 9^7mod 143 = 48 = C

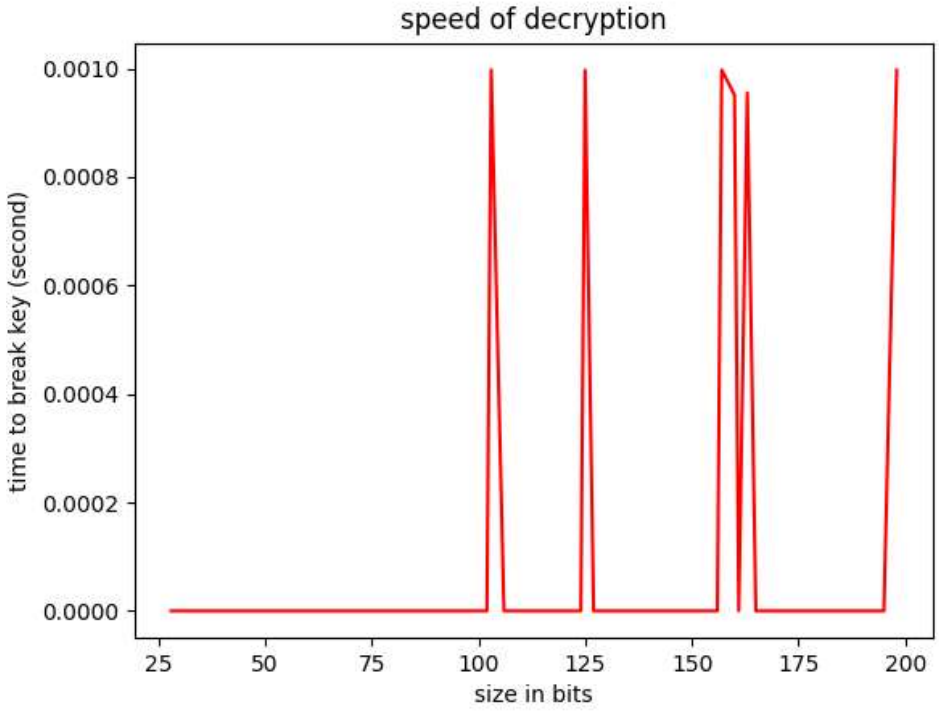
When Alice receives Bob's message, she decrypts it by using her RSA private key (d, n) as follows:

C^d mod n = 48^{103} mod 143 = 9 = M

Encryption/Decryption Analysis:

File:" speed_encryption_decryption"





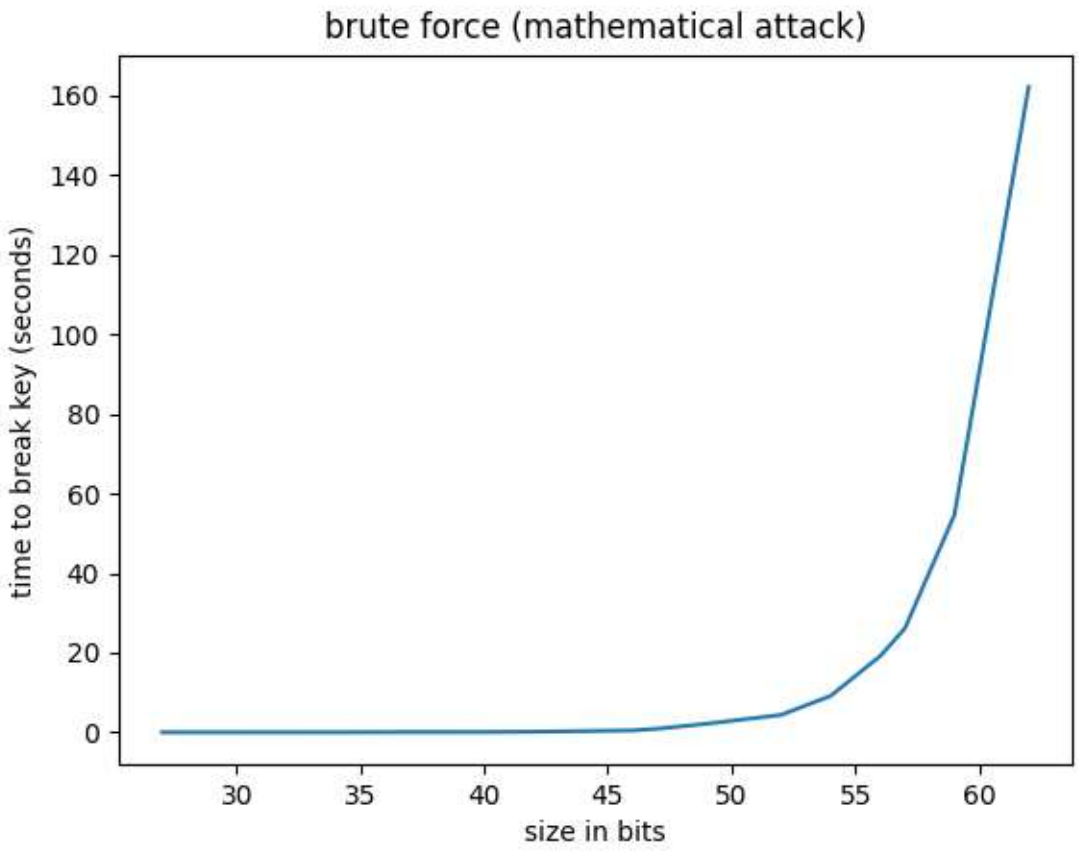
Key size doesn't affect Time of encryption and decryption [time almost zero] because algorithm has simple operations like addition and power …etc

Attack:

File: ” attak.py”

We have prime key w,n

First, we find prime factorial [P] to n than calculate q=n/.then , calculate phi_n =(p-1)*(q-1)
We can get d*e=1 mod phi_n. we get d then attackers have private key (p,q,d)



Time increases exponentially by increasing number of bits.