CSCI 650

Principle of Computer Security

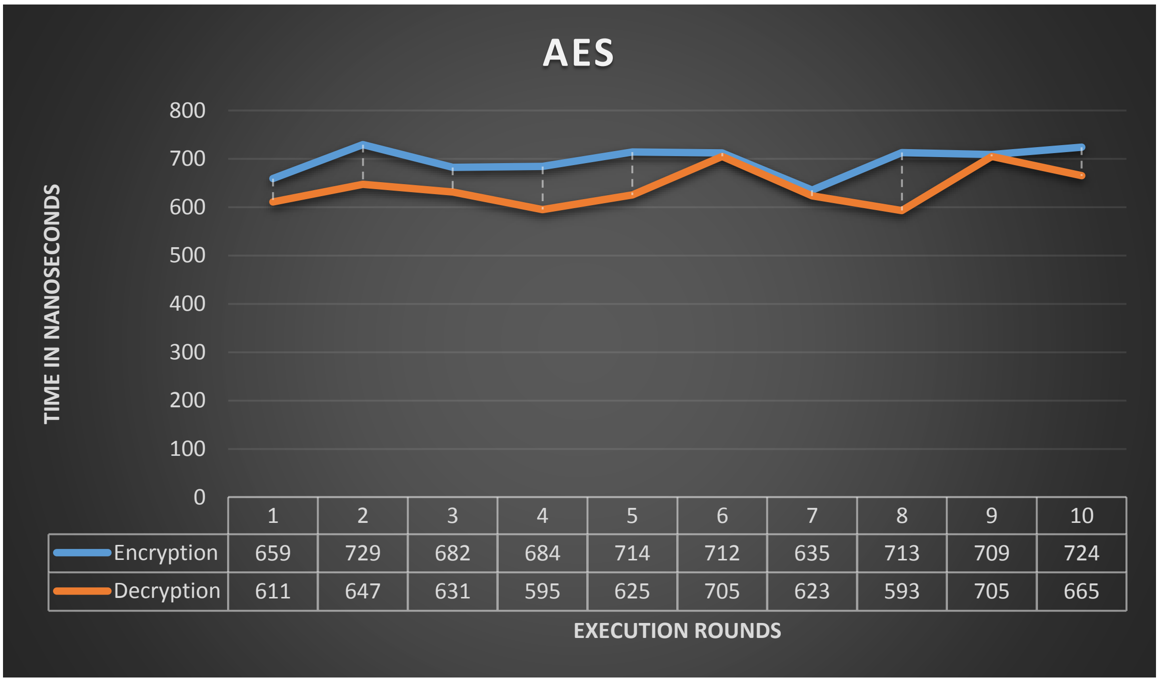
Assignment 2

Group 1
z1744852 - Gowrinath Jarugula
z1746938 - Aienampudi Raga Tapaswi
z1748613 - Doddi Vineel

REPORT

AES_128/ECB/Nopadding

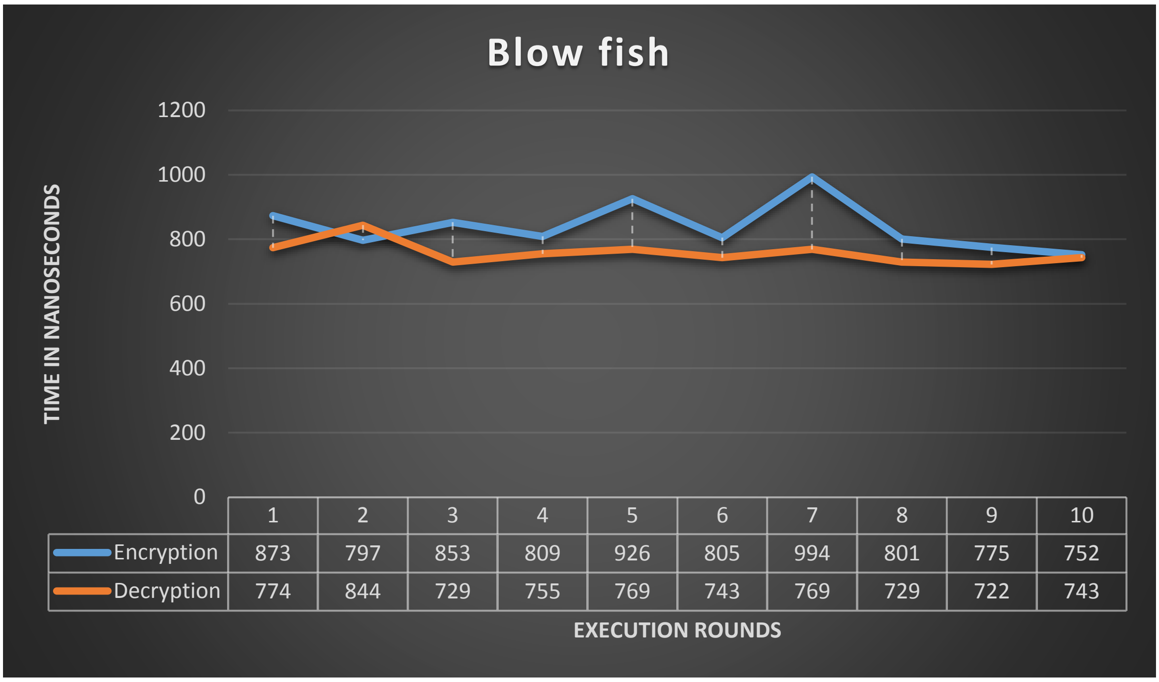
The encryption and decryption time for AES_128/ECB are almost very closer to each other with only a little difference. Here the AES/ECB only takes one block of data and the same block is encrypted and decrypted. In the case where we are using multiple blocks of data, encryption may appear slower that decryption as the encryption is done sequentially but the decryption can undergo parallel processing which saves system time.



	1	2	3	4	5	6	7	8	9	10
Encryption	659	729	682	684	714	712	635	713	709	724
Decryption	611	647	631	595	625	705	623	593	705	665

Blowfish

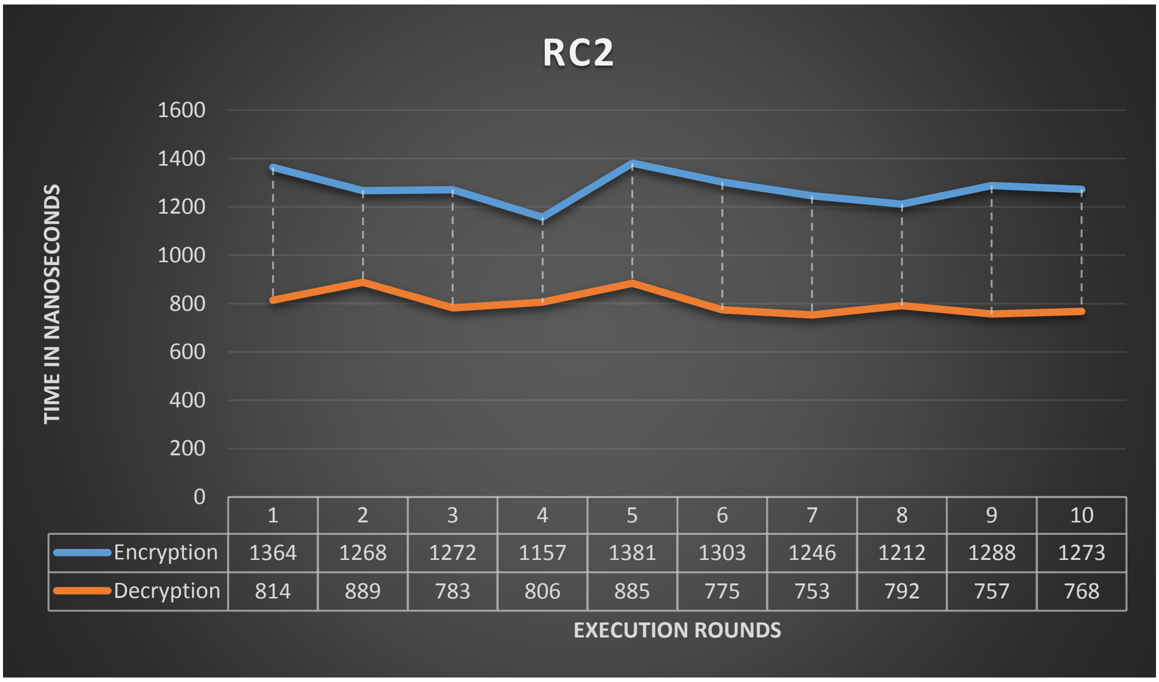
The blowfish is also a symmetric algorithm which uses variable key sizes ranging from 32 to 448. The above readings are for 128 bit key and 64 bit block size. Here also the encryption time is slightly elevated than the decryption time. The reason behind this is in most cases the blowfish key setup takes time. It creates 4 KB of table instances in the RAM which will slow up the encryption time.



	1	2	3	4	5	6	7	8	9	10
Encryption	873	797	853	809	926	805	994	801	775	752
Decryption	774	844	729	755	769	743	769	729	722	743

RC2

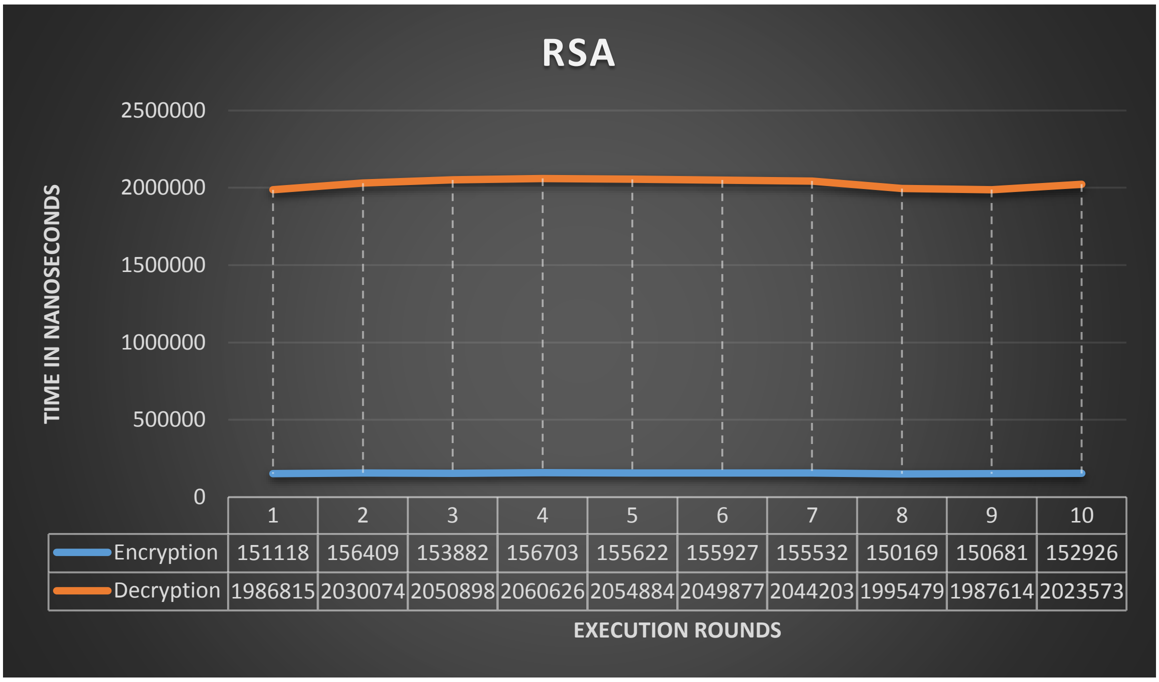
As most of the symmetric algorithms, RC2 algorithm also shows the time difference between encryption and decryption. The difference here is not small as of the other algorithms we had used. This is due to the Mixing and Mashing of the block during the encryption of the data. And the key setup also takes time as it generates an array of 64 16 bit round keys which takes up system time.



	1	2	3	4	5	6	7	8	9	10
Encryption	1364	1268	1272	1157	1381	1303	1246	1212	1288	1273
Decryption	814	889	783	806	885	775	753	792	757	768

RSA

The RSA algorithm is asymmetric algorithm. The above observations are for a key size of 1024 and block size of 128 and public key encryption and private key decryption. When we take a look at the times of the encryption and decryption there is a very big variation depending upon the key used. In general, the computational effort for encryption is proportional to n^2 and the decryption is proportional to n^3 where n is the key size. But this is not the complete scenario and we will discuss how the public and private keys effect this in the upcoming observations.



	1	2	3	4	5	6	7	8	9	10
Encryption	151118	156409	153882	156703	155622	155927	155532	150169	150681	152926
Decryption	1986815	2030074	2050898	2060626	2054884	2049877	2044203	1995479	1987614	2023573

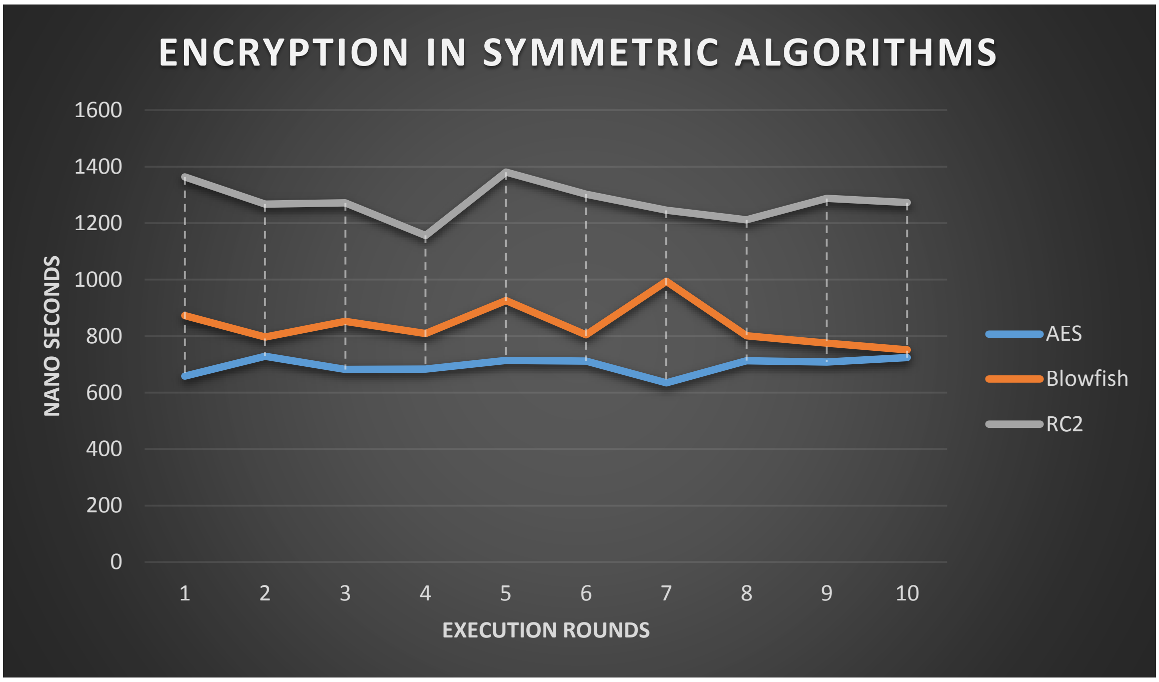
Encryption and Decryption in general

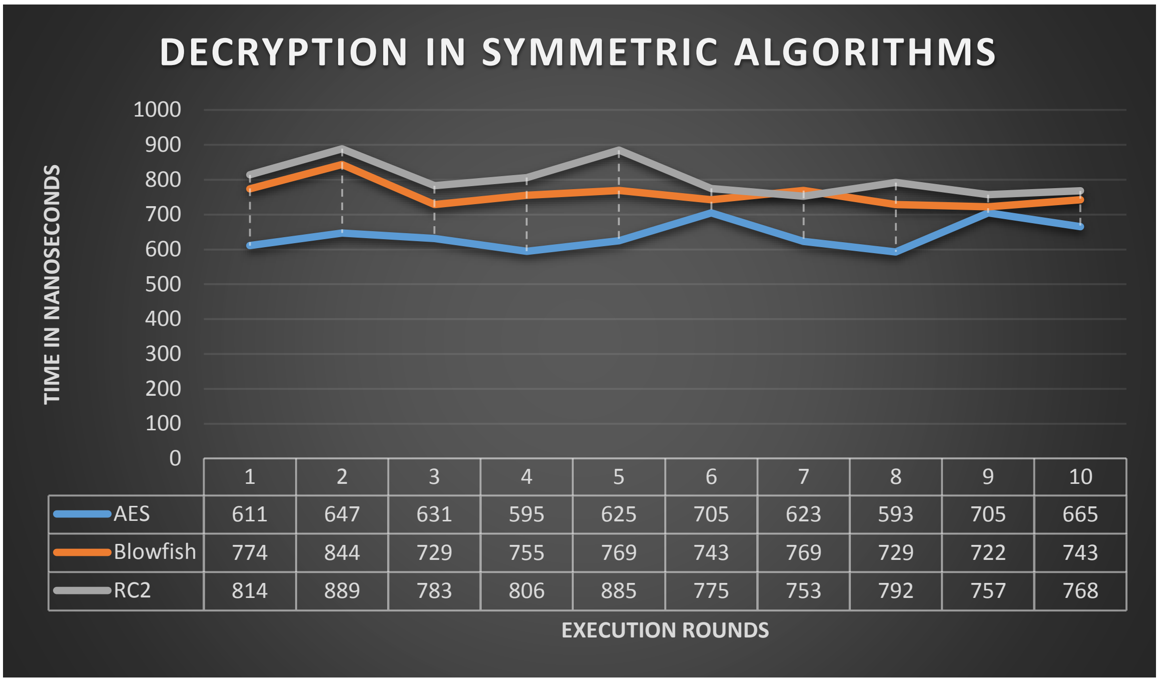
For symmetric algorithms,

Most of the algorithms have closer encryption and decryption times but from the observations we had so far shows that the encryption is slightly longer than the decryption. This delay can be explained as the encryption side takes up the time to setup the key and sometimes on how the data is accessed. The decryption already had the key and the cipher which it can access right away making it a bit quicker.

For asymmetric algorithms,

It is not possible to generalize timings in the case of asymmetric algorithms. As far as from the observations we had so far the encryption and decryption times depend on the keys used and their respective sizes. Longer keys often indicate longer time taken and hence taking up the system time.

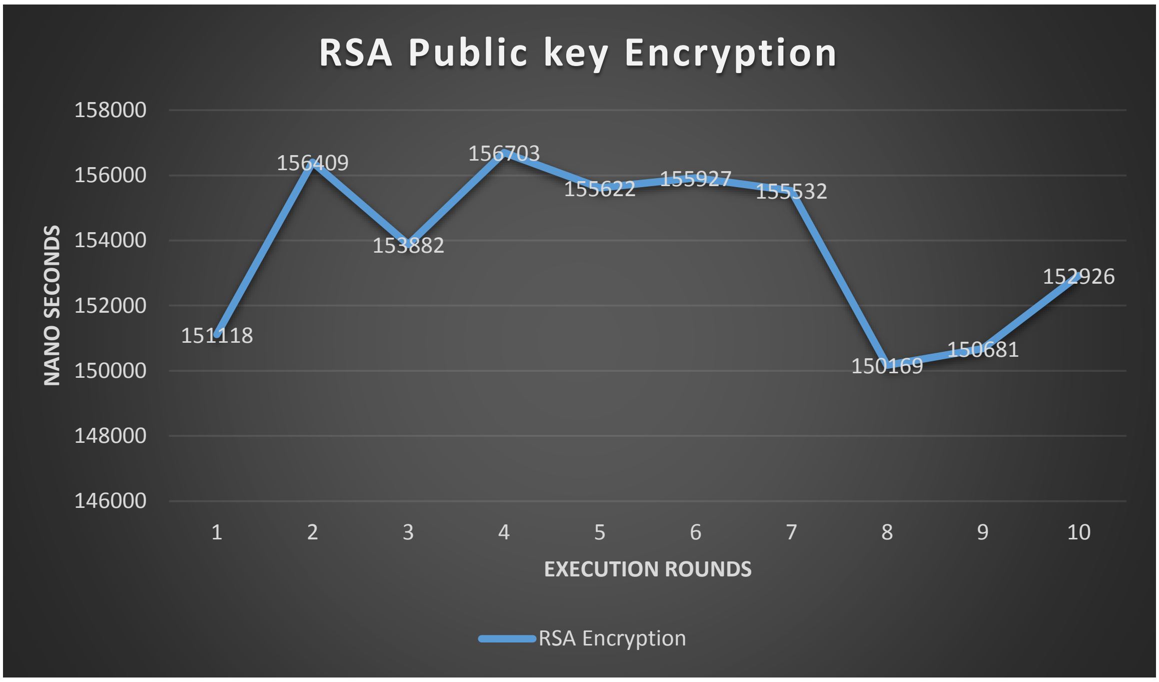




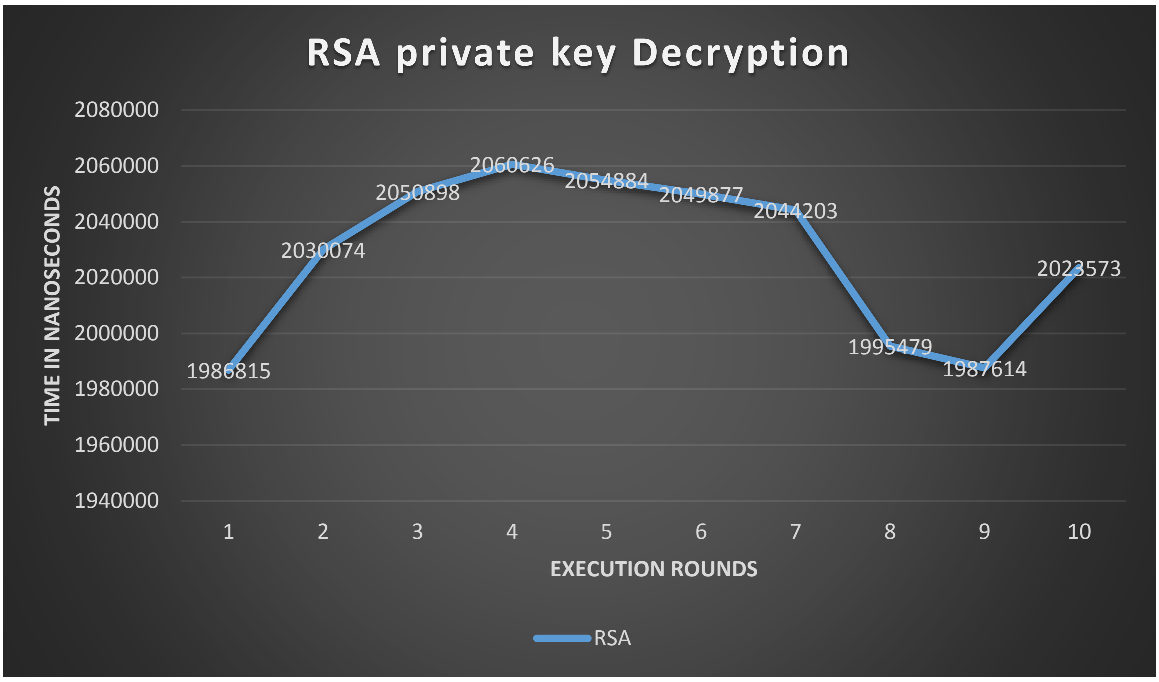
	1	2	3	4	5	6	7	8	9	10
AES	611	647	631	595	625	705	623	593	705	665
Blowfish	774	844	729	755	769	743	769	729	722	743
RC2	814	889	783	806	885	775	753	792	757	768

RSA Key Usage

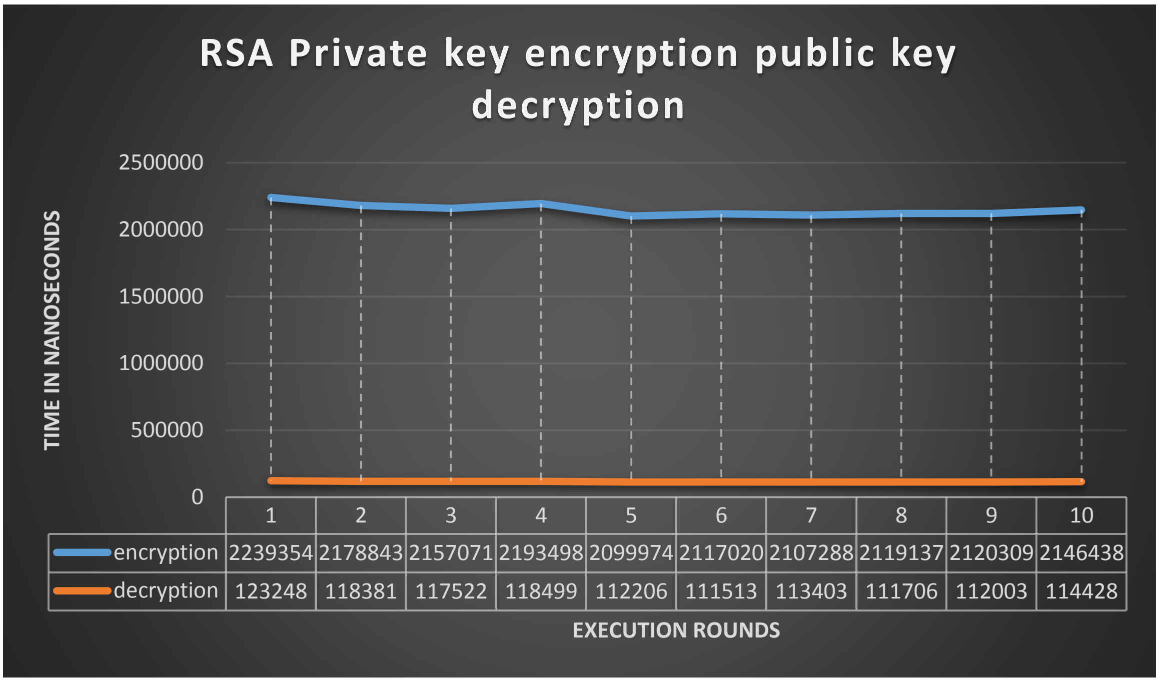
In RSA the public key and the private keys used plays a bigger role in the system time taken. The RSA private key is necessarily a large number when compared to that of the public key. The public can be any number of small size which takes up significantly less time when compared to that of larger private key. The following charts shows us various encryption and decryption times with varying public and private keys.



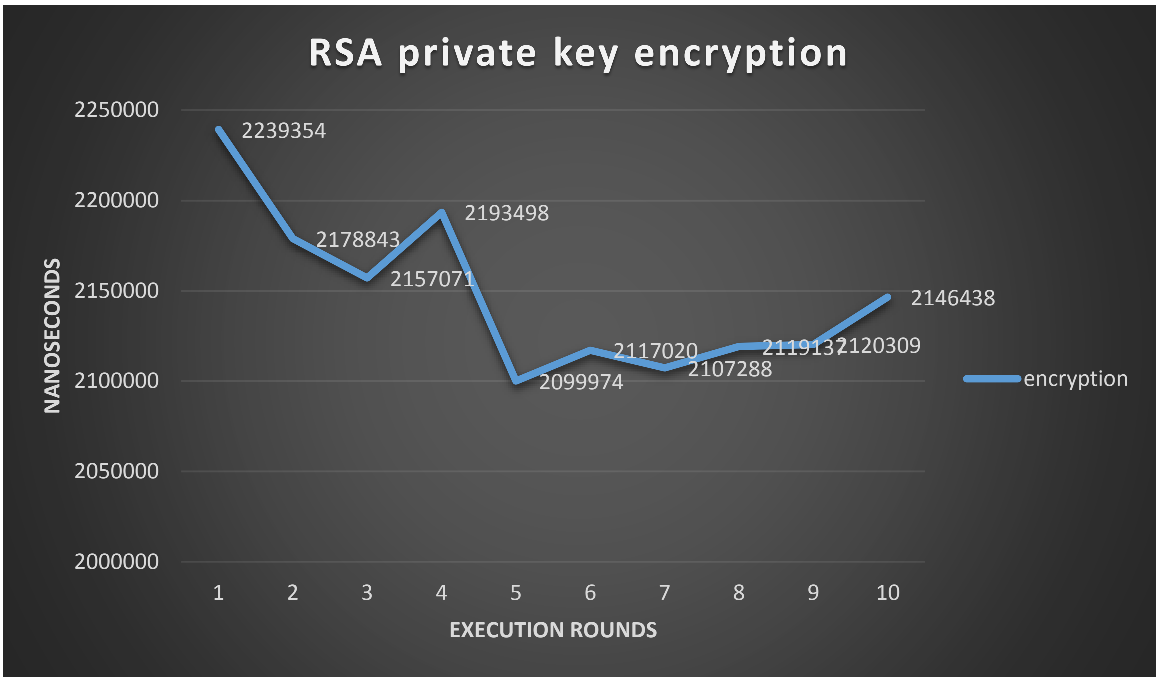
This chart and the next one shows the public key encryption and private key decryption. We can observe a significant difference in the times taken. The encryption took less time to that of decryption as we had used public key which is of smaller size to that of private key on decryption side.

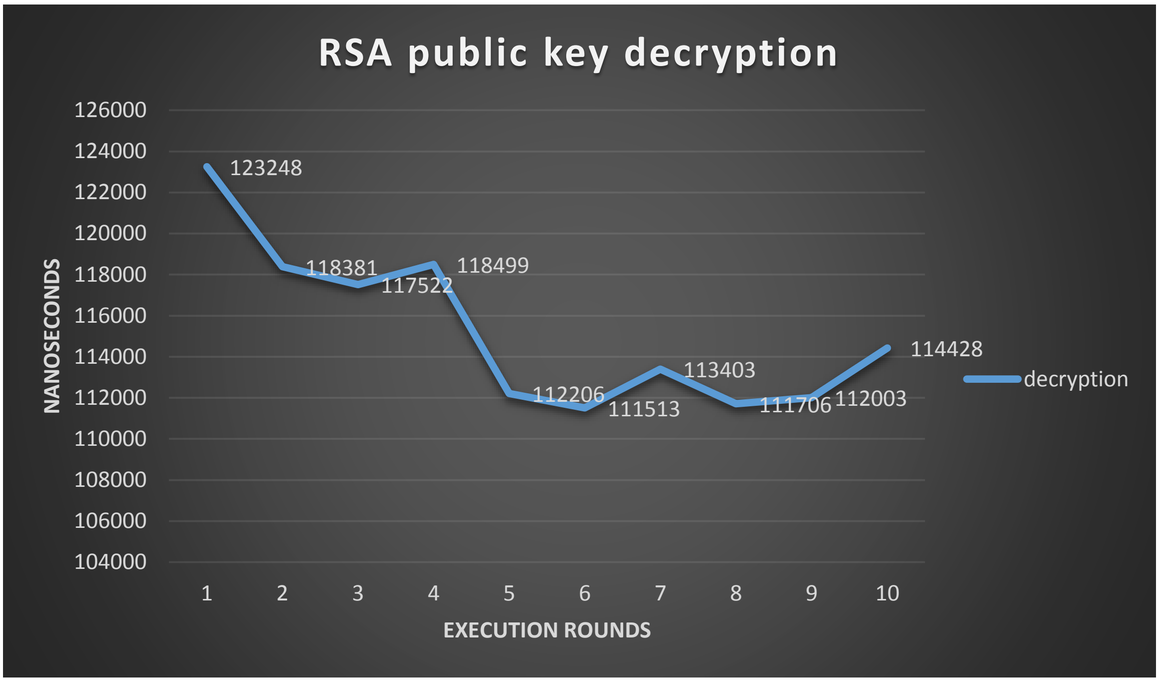


Now let’s look at the case where we use private key to encrypt and public key to decrypt. We can see that now the encryption took much time unlike the previous case.



	1	2	3	4	5	6	7	8	9	10
encryption	2239354	2178843	2157071	2193498	2099974	2117020	2107288	2119137	2120309	2146438
decryption	123248	118381	117522	118499	112206	111513	113403	111706	112003	114428





Observations from keys in RSA

From the observations we had so far, the side using the public key takes less time to that of the side using private key. This difference is mainly due to difference in sizes between the two keys. We are required to use both the public and private key. Using only one key on both sides will only lead to deciphering errors.

Symmetric vs Asymmetric

From the observations, it is clearly inferred that the symmetric and symmetric encryptions differ much in the case of encryption timings. The symmetric algorithms are much quicker in both encryption and decryption. This is mainly due to the asymmetric algorithms using two different keys one to encrypt and the other to decrypt which will take higher system time.

Note: *All the observations made are taken at the same time i.e., running one algorithm after the other without any other intermediate work on an I7 octa-core processor with 1.7GHz processor speed and 8 GB RAM. The virtual machine have the configuration of 9GB memory, 2 GB RAM and is given two cores. The algorithms are also tested on another I5 processor with the same RAM and only a slight increase in the values is observed.*