Benchmark Testing Asymmetric Cryptography Functions

## Contents

1 System Specifications

2 Environmental Specifications

3 Introduction

4 Keypair Generation

5 Encryption Using RSA

6 Decryption Using RSA

7 Digital Signing

8 Signature Verification

9 Conclusion

## 1 System Specifications

* Processor: AMD Ryzen 7 2700X
* GPU: NVIDIA GeForce RTX 2060
* Motherboard: MSI B450 TOMAHAWK MAX
* RAM: 8 GB x2
* Operating System: Windows 10

## 2 Environment Specifications

* Environment: Visual Studio Code
* Python: 3.10
* Cryptography Version: 2.21

## 3 Introduction

The objective of this document is to benchmark test a selection of asymmetric cryptography functions within Python’s “cryptography” package. This document shall detail the results and compare their effectiveness.

## 

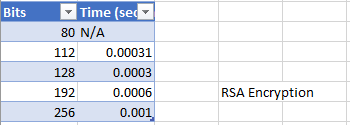
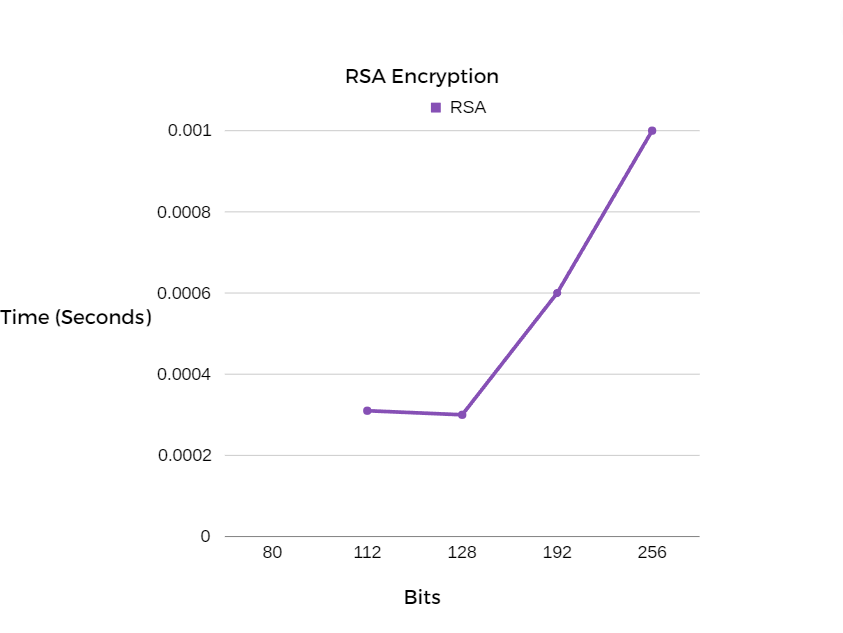
# 4 Keypair Generation

## 

In regards to keypair generation, it is clear that RSA is the most reliable. Not to say that the other functions are not useful, however. You will notice that DSA was actually more efficient for 80 bit and 112 bit key sizes, however it cannot process any key sizes bigger than that. ECC is definitely the fastest, generating a keypair in 0.009 seconds, although it can only process key sizes above 256 bits.

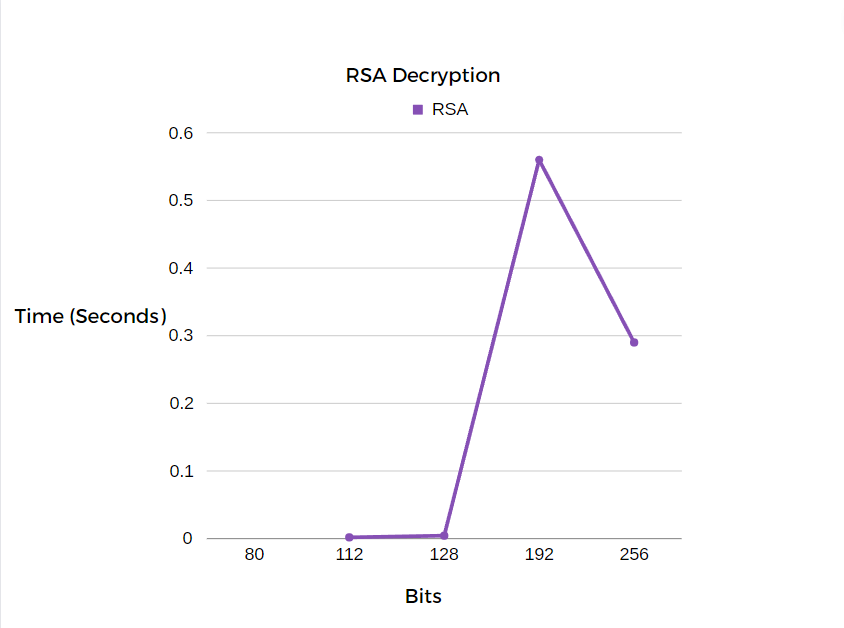
In conclusion, RSA is useful for key sizes of 128 or 192. DSA is useful for smaller key sizes, and ECC is useful for large key sizes.

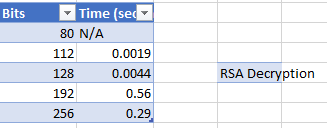
# 5 Encryption Using RSA



Encryption using RSA seen a relatively sharp incline in time taken as the bits increased

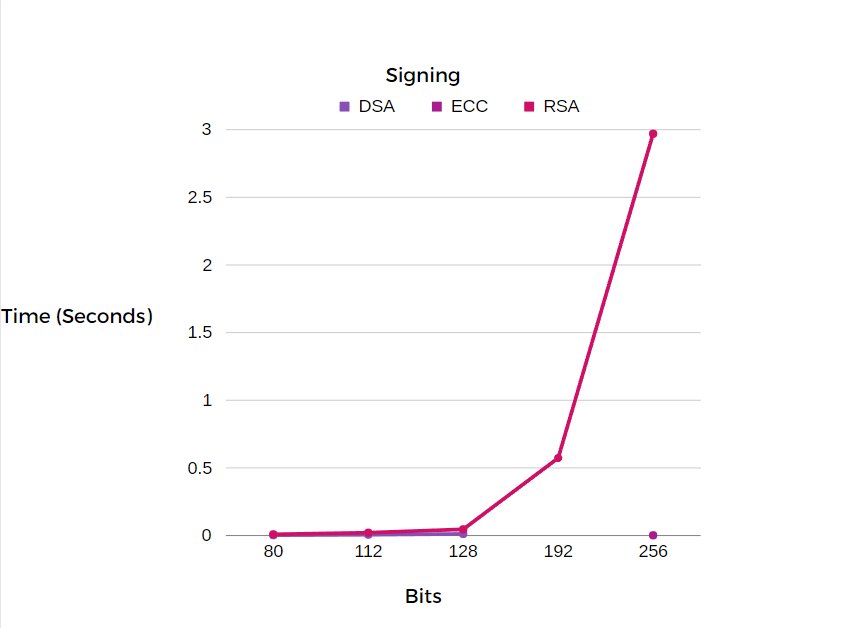
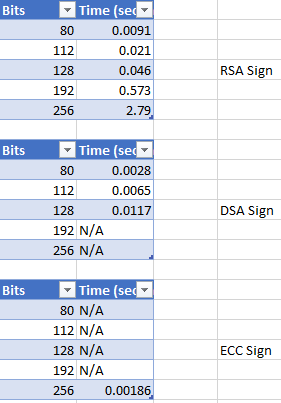
# 6 Decryption Using RSA





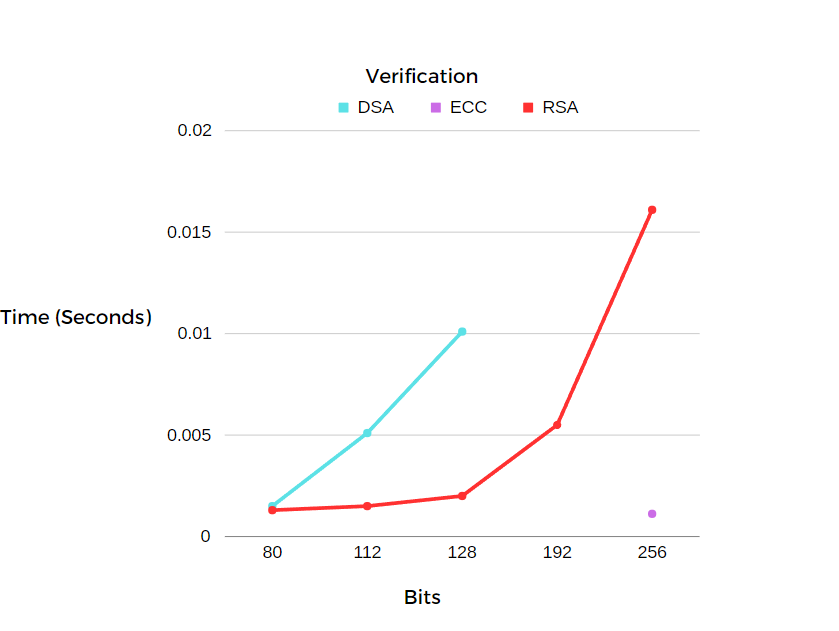
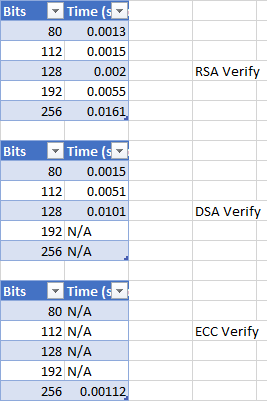
Decryption using RSA was interesting as 256 bits was actually almost twice as fast as 192 bits

# 7 Digital Signing

****

It is evident that RSA is the most reliable for creating digital signatures as it can do all bit sizes from 80 bits to 256 bits, however, when it is compared to ECC or DSA it is evidently slower.

# 8 Signature Verification

****

When it comes to signature verification, RSA is clearly the most reliable. Not only can it process all bit sizes, but it also appears to be faster than DSA. However, ECC is the fastest when it can be utilised.

# 9 Conclusion

It is safe to say that RSA is definitely the most reliable, however that isn't to say it is the best. DSA is typically better when dealing with smaller bit sizes, and ECC is better with larger key sizes. It is clear that each function has its use for certain situations.