SIL 765 - Network and System Security

Assignment - 2

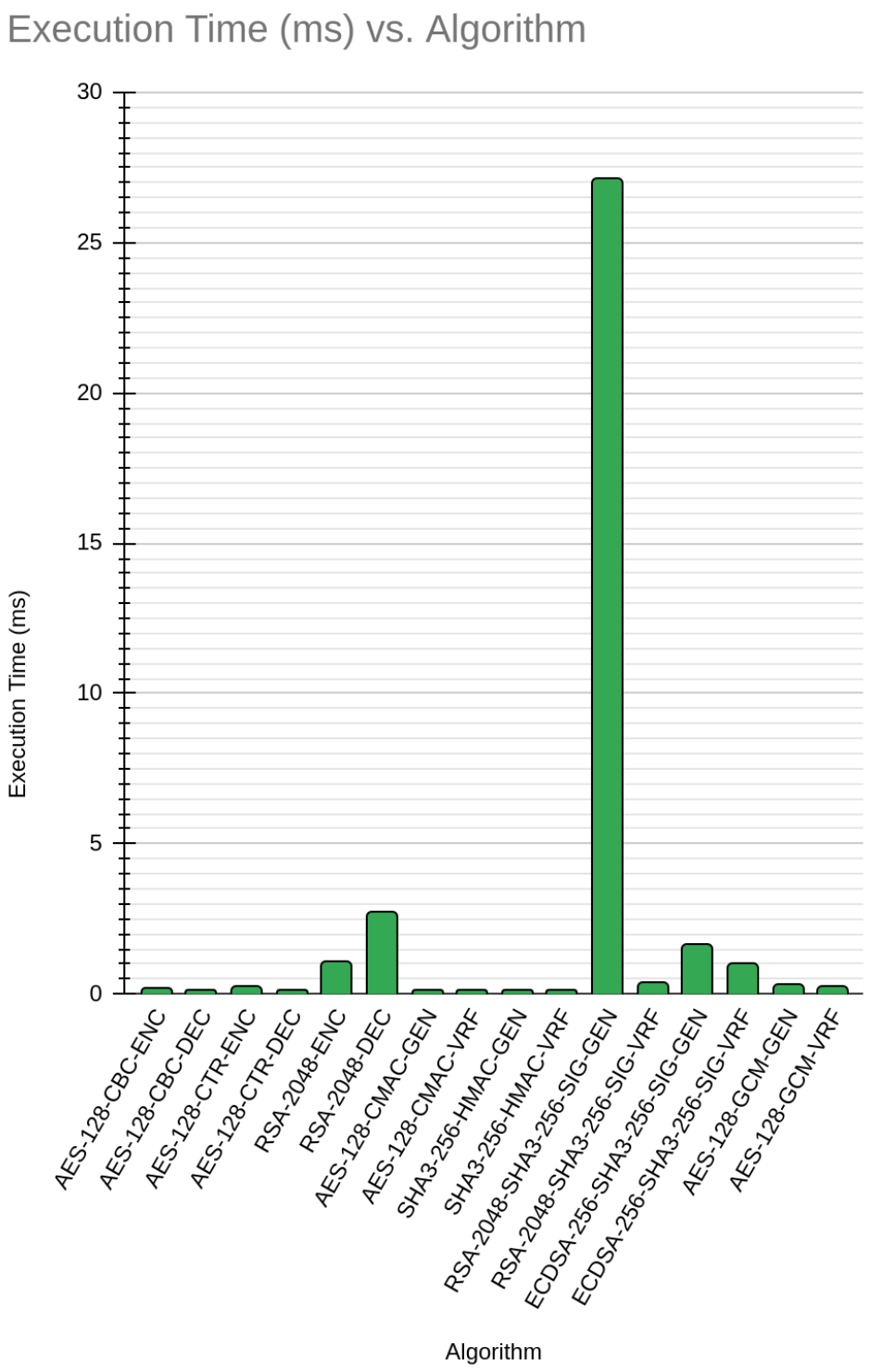
Name - Nutesh Kumar Sahu

Entry Number - 2021JCS2242

The Three Different Costs For Each Algorithm :

Algorithm	Key Length	Execution Time (ms)	Packet Length (Bits)
AES-128-CBC-ENC	128	0.1792	5120
AES-128-CBC-DEC	128	0.1332	
AES-128-CTR-ENC	128	0.2332	5064
AES-128-CTR-DEC	128	0.1244	
RSA-2048-ENC	2048	1.0297	2048
RSA-2048-DEC	2048	2.691	
AES-128-CMAC-GEN	128	0.1137	520
AES-128-CMAC-VRF	128	0.0994	
SHA3-256-HMAC-GEN	128	0.0975	648
SHA3-256-HMAC-VRF	128	0.0829	
RSA-2048-SHA3-256-SIG-GEN	2048	27.1418	2528
RSA-2048-SHA3-256-SIG-VRF	2048	0.3769	
ECDSA-256-SHA3-256-SIG-GEN	256	1.6264	1216
ECDSA-256-SHA3-256-SIG-VRF	256	1.0194	
AES-128-GCM-GEN	128	0.3245	256
AES-128-GCM-VRF	128	0.2234	

Analysis of Execution Time :



From the above chart we can see that RSA takes a longer time to execute than all other algorithms.

Advantages and Disadvantages of Given Algorithms :

Algorithm	Advantages	Disadvantages
AES-128-CBC	1. It provides error multiplication properties 2. It uses chaining 3. It provides parallelization for decryption 4. If there is duplicate data in plaintext, it is not reflected in ciphertext	1. It is slower than other AES modes 2. It does not provide parallelization in encryption 3. Implementation of decryption is needed. 4. If there are wrong blocks, it will affect all following blocks
AES-128-CMAC	1. It works better if embedded hardware is involved	1. It is slower than HMAC
AES-128-CTR	1. It provides parallelization 2. It is based on stream cipher 3. It allows arbitrary message length 4. In this mode, decryption Implementation is not needed 5. No padding is required 6. If there are bad blocks, it will only affect the current blocks	1. It does not provide error multiplication properties
AES-128-GCM	1. It provides confidentiality 2. It provides integrity 3. It is a high-speed algorithm 4. It provides parallelization	1. It is very complex 2. High computation power required
RSA-2048	1. It provides safer encryption 2. It is simpler to implement 3. It is most widely used	1. The key length is high
ECDSA-256-SHA3-256	1. It requires shorter keys than RSA 2. It shows better performance than RSA	1. It is more complex to implement
RSA-2048-SHA3-256	1. It provides safer encryption 2. It is simpler to implement 3. It is most widely used	1. The key length is high
SHA3-256-HMAC	1. It generates a unique token for each request 2. It is easy to implement 3. It is ideal for a high performance system like routers 4. It provides higher security than a digital signature	1. It uses the symmetric key 2. key exchange is a problem