SIL765
Assignment – 2

Evaluating Cryptographic Primitives

COST ASSOCIATED WITH EACH ALGORITHM :-

Algorithm	Key Length (in bits)	Execution Time (in ms)	Packet Length (in bits)
AES-128-CBC-ENC	128	2.352	5120 (Plaintext = 5072 bits)
AES-128-CBC-DEC	128	0.308	
AES-128-CTR-ENC	128	2.460	5120 (Plaintext = 5072 bits)
AES-128-CTR-DEC	128	0.297	
RSA-2048-ENC	2048	5.425	2048 (Plaintext = 128 bits)
RSA-2048-DEC	2048	3.533	
AES-128-CMAC-GEN	128	4.542	256 (Plaintext = 5072 bits)
AES-128-CMAC-VRF	128	0.656	
SHA3-256-HMAC-GEN	128	2.513	512 (Plaintext = 5072 bits
SHA3-256-HMAC-VRF	128	0.544	
RSA-2048-SHA3-256-SIG-GEN	2048	5.653	2048 (Plaintext = 128 bits)
RSA-2048-SHA3-256-SIG-VRF	2048	1.856	
ECDSA-256-SHA3-256-SIG-GEN	256	4.043	512 (Plaintext = 5072 bits)
ECDSA-256-SHA3-256-SIG-VRF	256	2.866	
AES-128-GCM-GEN	128	2.897	128 (Plaintext = 5072 bits)
AES-128-GCM-VRF	128	0.916	

FINDINGS :-

General :-

--> Decryption always takes less time than encryption in all the algorithms given.
--> Verification of authentication tag always takes less time than authentication tag generation in all the algorithms given.

Discussions of each algorithm :-

1. AES-128-CBC :

1. Implementation of it is easy and parallel decryption is supported, hence most commonly used.
2. With CBC mode, identical blocks do not have the same cipher as the initialization vector adds a random factor to each block; hence, why the same blocks in different positions will have different ciphers.
3. Its encryption is not tolerant of block losses. This is because blocks depend on their previous blocks for encryption.
4. Encryption of blocks needs to be done sequentially, not in parallel.

5. Much better than RSA in terms of key length and execution time.
6. CBC is not an authenticated encryption mode. Any unauthenticated encryption is theoretically vulnerable to Chosen Ciphertext Attacks (CCA)
7. AES-CBC on its own does not provide proof that the ciphertext has not be tampered with by an attacker

2. AES-128-CTR:

1. Saves time by giving the benefit of preprocessing.
2. Parallelisation for encryption and decryption is supported.
3. Random access of plaintext is also supported.
4. CTR mode has CPA security.
5. Much better than RSA in terms of key length and execution time.

3. RSA-2048 :

1. Safe and secure as complex mathematics is used.
2. Takes more time and space than the other algorithms.
3. Third party is needed to verify the public keys.
4. Key length is too long.
5. RSA algorithm uses the public key to encrypt data and the key is known to everyone, therefore, it is easy to share the public key.
6. Fast public key operations and direct encryption possible.

4. AES-128-CMAC :

1. Key length is larger than SHA3-HMAC.
2. Execution time and packet size is less than SHA3-HMAC.

5. SHA3-256-HMAC :

1. Due to the quick calculations of the hash functions it is best suited for high performance systems like routers.
2. HMACs provide comparable security to digital signatures despite the fact that digital signature are larger, which makes it strong and cost-effective.
3. A secure one-way function is provided by SHA-3.
4. It uses shared key which may lead to non-repudiation.

6. RSA-2048-SHA3-256-SIG :

1. It is the industry standard for public key cryptography from a long time now. It was introduces in 1994.
2. Key length required is more that ECDSA still the level of security is comparable to ECDSA
3. RSA appears to be substantially quicker than ECDSA in most realistic implementations when checking signatures, however it is slower when signing.

7. ECDSA-256-SHA3-256-SIG :

1. It came into use quite recently. It was introduces in 2008.
2. Key length required is less than RSA to provide the same level of security as RSA.
3. ECDSA is slower than RSA in realistic implementations.

8. AES-128-GCM :

1. The algorithm fails if if a nonce is reused. A forged ciphertext can be easily created if a nonce is reused.
2. Nonce are short which makes it vulnerable.
3. Due to the first point, integrity and confidentiality are violated.
4. Its hardware implementation can achieve high speeds with low cost.
5. GCM is proven secure in the concrete security model

SUBMITTED BY :-

- Nikita Bhamu
- 2018CS50413