There are a limited number of reliable hybrid cryptosystems that can be used to protect intelligent IoT devices, especially in smart cities, smart hospitals, smart homes and industrial fields. The goal is to achieve a trade-off between performance and security in these limited environments and to achieve a more secure hybrid cryptosystem with high performance requirements. The results show that the proposed hybrid cryptosystem, which links ECC and XXTEA, provides better security and higher performance than RSA and XXTEA with 40%. He have the ability to protect intelligent IoT devices against online attacks. He can effectively achieve confidentiality, authenticity, honesty and non-repudiation. Comparative analysis and evaluation were carried out; therefore, a strong hybrid cryptosystem has been proposed. Uses a chaotic theory to generate random keys. The analysis included the most important factors to be measured when using lightweight ciphers to adapt to the limited resources of intelligent IoTs. Among these factors are the level of security, memory size, power consumption, encryption time, decryption time and bandwidth.

The elliptic curve cryptography (ECC) is asymmetric cryptography engages the use of two keys. A private key used to decrypt messages and sign (create) signatures. And a public key used to encrypt messages and verify signatures. ECC is used to achieve authenticity, integrity, and non-repudiation with the help of some additional algorithms. ECDHE Digital signatures are used to verify the authenticity of messages and confirm that they have not been altered in transmission. To assure the integrity of the received data, a hashing algorithm is used. The Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm uses ECC to provide a variant of the Digital Signature Algorithm (DSA). A pair of keys (public and private) are generated from an elliptic curve, and these can be used both for signing or verifying a message’s signature.

The hybrid cryptosystem proposed consists of three main components including the XXTEA (symmetric block cipher) used to achieve confidentiality, the ECC (asymmetric cipher) used to achieve authenticity, integrity and non-repudiated based digital signature, and the chaotic keys generator used to generate random keys. The aim is to achieve the best performance with a high level of security. The Chaotic systems (Chaos) [34] are used to generate random keys. It has the following advantages.

Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices

1. The Chaotic sequences are nonlinear systems that are inevitable.

2. They are very sensitive to change in initial value or seed value.

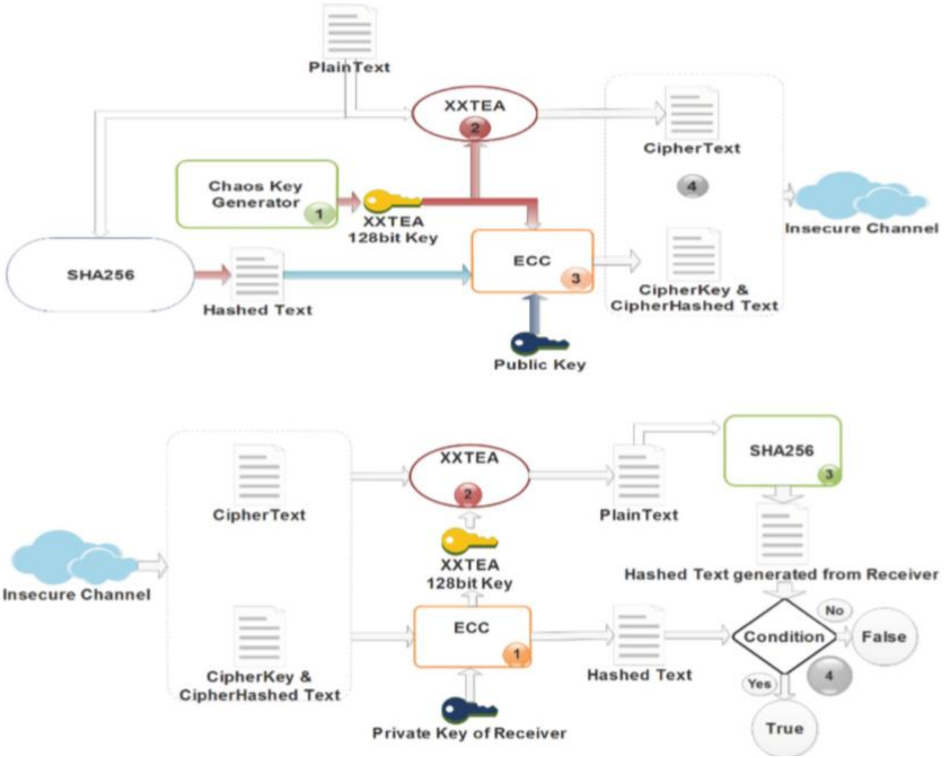
3. Two isomorphic chaotic systems with exact distinctions in seed values will produce two totally different chaotic sequences within a short period of time.

4. The strings given by chaotic systems are not only random but regenerative.

Because of these features, chaotic equations can be used to implement the key generator in cryptography. Some examples of chaotic equations are sine map, tent map, and Logistic map. One of the most common utilizing is the logistic map that can be given by

$$X_{n+1} = 1 - 2X_n^2;$$
$$X_n \; ranges\,from \quad -1 \; to \; 1 \; and \; n = 0, \; 1_{,\ldots}$$

Figure 1a and b show the component used to implement the hybrid cryptosystem proposed. The following algorithm illustrates the steps of operations of the hybrid cryptosystem.


PlainText
XXTEA
2
CipherText
Chaos Key Generator
1
XXTEA 128bit Key
4
Insecure Channel
SHA256
Hashed Text
ECC
3
CipherKey & CipherHashed Text
Public Key
CipherText
XXTEA
2
PlainText
SHA256
3
Insecure Channel
XXTEA 128bit Key
Hashed Text generated from Receiver
CipherKey & CipherHashed Text
ECC
1
Hashed Text
Condition
No
False
4
Yes
True
Private Key of Receiver