International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

XOR Cipher

Samriddhi V[1], Sanjana[2] , Shalini C[3], Sinchana A[4], Suma V Shetty[5]

[1,2,3,4,5]Department of Electronics and Communication Engineering
Sapthagiri College of Engineering, Bengaluru, India
Affiliated to Visvesvaraya Technological University, Belagavi, India

Abstract:
The XOR cipher is a simple symmetric encryption algorithm based on the (XOR) logical operation. It is broadly used in cryptography, data masking, and lightweight encryption applications due to its simplicity and efficiency. The XOR cipher operates by applying the XOR function between the plaintext and a key, ensuring that the encrypted output appears random. The same XOR operation is used for decryption when the ciphertext is XORed with the same key, restoring the original plaintext. Despite its efficiency and ease of implementation, the XOR cipher is vulnerable to attacks if the key is short ,predictable, or reused.However,it forms the foundation for more complex encryption schemes, such as stream ciphers and one- time pad encryption. Due to its lightweight computational requirements ,the XORcipheris often used in embedded systems, secure communication protocols, and hardware security applications. This paper explores the implementation ,advantages, and limitations of the XOR cipher, highlighting its role in modern cryptographic systems. It is the core principle behind the OTP, the only theoretically unbreakable encryption method when used with a truly random key of the message.

Keywords: XORCipher, Cryptography, Lightweight Encryption, Bitwise Operation,IOT Security

1. Introduction

XOR(Exclusive OR), is fundamental in computer science and digital electronics. It's also crucial in encryption algorithms, offering a unique way to protect data from unauthorized access. Before diving into cryptography, it's essential to grasp the basics of XOR. XOR operation is a fundamental logic function that processes two binary values,producing an output of 1 when the inputs are different and 0 when they are identical. XOR, short for exclusive OR, is a fundamental concept in computer science and mathematics. It is used extensively in various or XOR (Exclusive OR) cipher is a simple and widely used encryption technique. It works by performing a bitwise XOR operation between the plain text message and a secret key.decrypting the encrypted message requires performing another XOR function using the same key .However,issues such as Single Event Upsets(SEUs) can cause errors in logic processing,which may affect the systems reliability

XOR (Exclusive OR), is fundamental in computer science and digital electronics. It's also crucial in encryption algorithms, offering a unique way to protect data from unauthorized access(taken from paper [2]). Before diving intocryptography, it'sessentialtograspthebasicsofXOR. XOR is a logical operator that takes two binary inputs and returnsabinaryoutput.Theresulting outputistrue(1) onlyif the inputsdiffer; otherwise, it is false (0). XOR, short for exclusive OR,is a fundamental conceptin computer science and

mathematics. It is used extensively in various or XOR (Exclusive OR) cipher is a simple and widely used encryption technique. It works by performing a bitwise XOR operation between the plaintext message and a secret key. The resulting ciphertext message can be decrypted by performing another XOR operation with the same key..

2. Objectives

1. Simplicity:The XOR cipher is one of the simplest encryption techniques available. It only requires:

- Aplaintextmessage
- Akeyofanylength
- TheXORoperation

2. Lightweight Encryption: Since XOR operations are computationally inexpensive, theXOR cipher is useful in

- Embeddedsystems
- IoT(InternetofThings)devices
- Simpledatamaskingapplications

In contrast to advanced encryption methods like AES or RSA,XOR encryption demands minimal computing resources and memory.This efficiency makes it particularly suitable for environment with limites processing power.

3. problem statement

- Attacks such as side- channel attacks, differential attacks. A one-size- fits-all lightweight cipher may not meet diverse application needs.
- The cipher is designed to be efficient in terms of resource usage,making it suitable for devices with limited processing power.
- A32-bitstorageisanalternativemethodused.

4. proposed frame work

A SOFTWARE TOOLS USED

CADENCETOOL

1. DIGITAL DESIGN AND IMPLEMENTATION:
   Genus Synthesis Solution:You'd use Genus to translate the high-level description of your XORcipher(likely in RTL Verilog or VHDL) into a gate-level netlist
2. CUSTOM/ANALOGDESIGN:
   Virtuoso Platform:This includes schematic capture, simulation, and layout.
3. VERIFICATIONANDANALYSIS:

Tempus Timing Sign off Solution:This is critical for the cipher to operate correctly at its intended speed

B. IMPLEMENTATION

1. UNDERSTANDINGTHEXORCIPHER

The XOR cipher is a simple encryption technique where:

- Encryption:Ciphertext=Plaintext⊕Key
- Decryption:Plaintext=Ciphertext⊕Key

2. DESIGNFLOWUSINGCADENCETOOLS

Step	Cadence Tool	Purpose
RTL Design	Genus	Writing Verilog description
Simulation	Xcelium	Verifying functionality
Synthesis	Genus	Converting RTL to gate-level netlist
Physical Design	Innovus	Layout and optimization
Verification	Innovus	DRC, LVS, and timing checks

3. RTLDESIGN

- Specify the plaintext , key, andciphertextas32-bit signals.
- Implement an XORoperation to perform encryption.

4. FUNCTIONALVERIFICATION

- Develop a test bench to verify encryption and decryption.

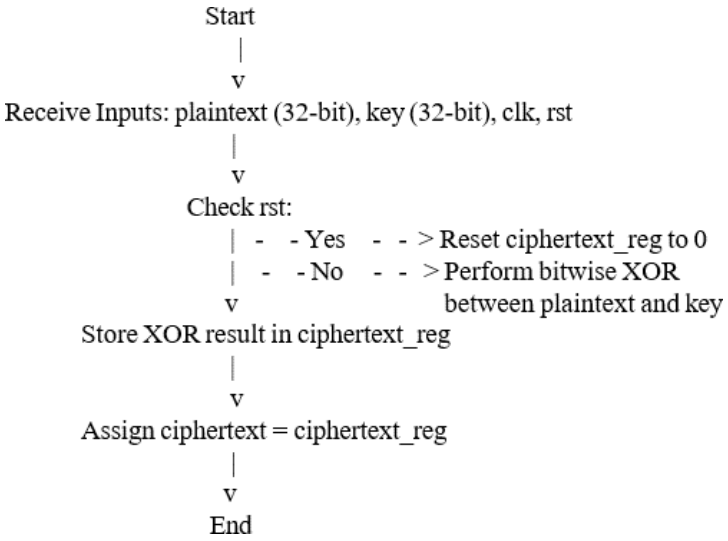
5. SYNTHESIS

- Setup timing constraints(e.g.,clock frequency, delay requirements).
- Run synthesis to convert the RTL design into a gate-level netlist using standard cells.

*C.*ENCRYPTIONPROCESS

The encryption process(i) has the following steps:

- Step-1:Read the complete plaintext byte by byte or read each 8-bit ASCII character from the full string 'n‟ bit of plain text from LSB.
- Step-2:Based on the size of plaintext, apply the Encryption key value of 'n'bit.
- Step-3:Accomplish the bit wise XOR operation on plaintext and encryption key value.
  Step-4:Read the corresponding binary value as cipher text.
- Step-5:Perform the step-1tostep-4operationtillEnd of File (EoF) is completed.



Figi: shows encryption process

D.DECRYPTIONPROCESS

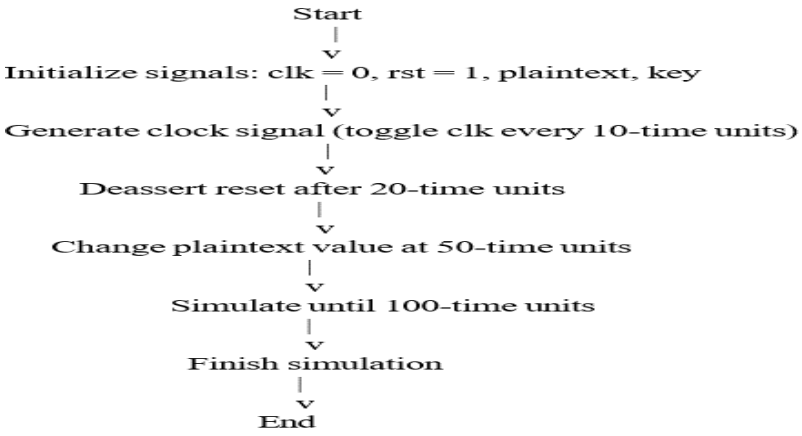
The decryption process(ii)has the following steps:-

Step-1:Readthe8-bitASCIIvalueofeachcharacter for 'n' bit cipher text encoded at Transmitting end.

Step-2:Based on the size of plaintext and ciphertext, apply the decryption key value of n' bit.

Step-3:Accomplish the bitwise XOR operation on cipher text and decryption key value

Step-4:The decoded binary value at the receiving end is original plain text of "n bit" which is read against 8-bit ASCII value as original character till End of File (EoF)is completed.The decoded text is the original text sent on transmitting end.



Figii: shows decryption process

5. Result

Plaintext waveform transitioningto1,then0,then1,then1.
Key waveform transitioning to 0, then 1, then 1, then 0. Ciphertext wave form transitioning to1,then1,then0,then 1, matching the XOR result

6. Conclusion

The key features are Simplicity and efficient,Fast encryption and decryption, and minimal energy usage. The XOR Cipher Circuit is suitable for secure data transfer in applications that do not require high level of security.
The circuit utilizes the bitwise XOR operation to encrypt and decrypt data.
32 Bit is used to increase its performance and storage capacity.The XOR Cipher Circuit is a valuable resource for educating students on digital logic and cryptography concepts.

Refernces

1. Abdul AlifZakaria etal.,[1]proposed a“Trend analysis on the design of lightweight block cipher”, 2016 IEEE I n t e r n a t i o n a l Conference on Computational Intelligence and Computing Research(ICCIC), Chennai, India, 2016, pp. 1-3,10.1109/ICCIC.2016.
2. Appala Naidu Tentu [2]“Development of symmetric-key block cipher structures”,2021 6th International Conference on Communication andElectronicsSystems(ICCES),Coimbatore,India,2021,pp.972-976,Doi: 10.1109/ICCES51350.2021.9489097.
3. Sarvar Patel et al.,[3] proposed Ciphers: “Role of nonlinearcomponents in block cipher “,2015 International Conference on Advances in Computer Engineering and Applications,Ghaziabad,India, 2015, pp. 683-687, Doi: 10.1109/ICACEA.2015.7164778.
4. GeorgeHatzivasilisetal.,[4]"Fast Implementation of SimeckFamilyBlock Ciphers Using AVX2," 2018 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South),2018, pp. 1-6, Doi: 10.1109/PlatCon.2018.8472759.