LASAGNA REPORT

SECURITY PROJECT

PREPARED FOR :

First deliverable
27/04/2025

GROUP:

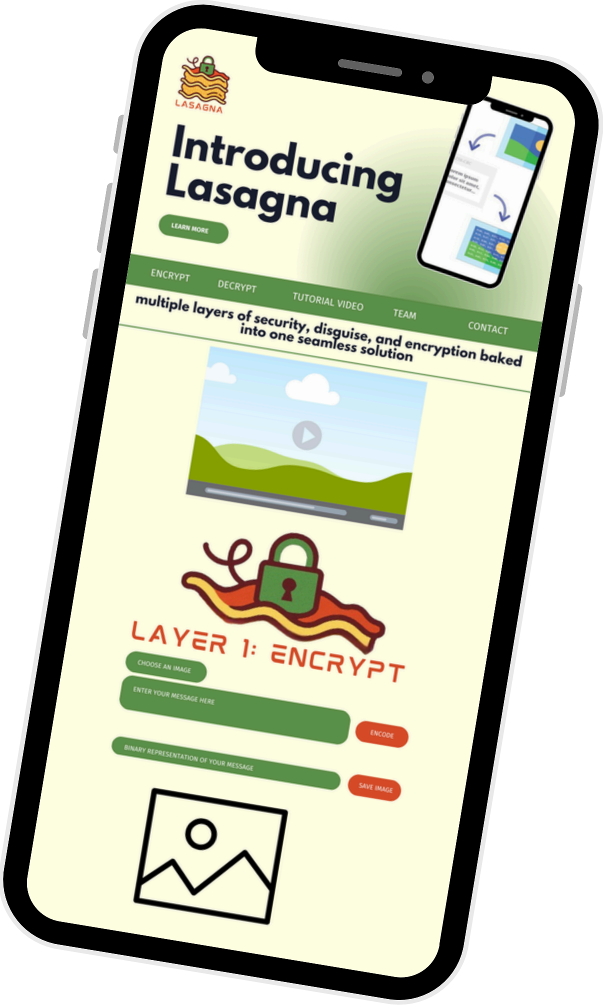
Rouaida Hentati
Hadil Mabrouk
Arij Khlif
Takwa Dalensi

TABLE OF CONTENTS

INTRODUCTION

In a world where digital privacy is increasingly threatened, protecting sensitive information is more critical than ever. LASAGNA offers a novel security solution that combines encryption, steganography, and obfuscation into a unified, layered defense. Its innovative approach ensures that private information's content and existence remain exceedingly difficult to detect or retrieve without authorization.

LASAGNA



Introducing Lasagna

multiple layers of security, disguise, and encryption baked into one seamless solution

LAYER 1: ENCRYPT

MAIN CONCEPTS

No. 01 – **Binary Conversion**

each character is converted to its ASCII code, then to binary.

No. 02 – **Obfuscation**

Obfuscation further strengthens security by introducing random or misleading data to confuse attackers and create uncertainty, ensuring the file appears entirely normal and meaningless.

In LASAGNA , noise is added to the carrier file making detection of hidden data even more difficult through statistical or forensic analysis.

No. 03 – **Encryption**

Encryption transforms readable information (plaintext) into an unreadable format (ciphertext) using an algorithm and a secret key.

In LASAGNA , encryption is performed using the XOR cipher where each bit of data is combined with a key bit following the One-Time Pad model for perfect secrecy.

Formula:

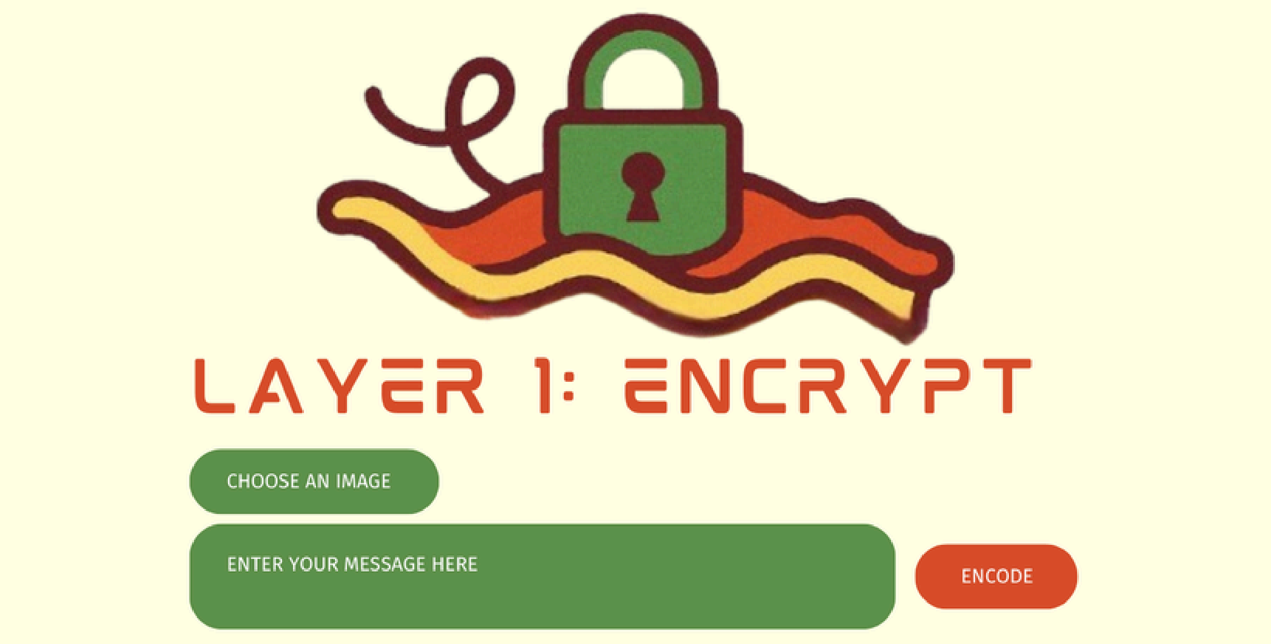
- $\text{Ciphertext}=\text{Plaintext}\oplus\text{Key}$
- $\text{Plaintext}=\text{Ciphertext}\oplus\text{Key}$

No. 04 – **Steganography**

While encryption scrambles the content, steganography embeds a message within innocuous files, like documents, films, or photos, to hide its very existence.

In LASAGNA , the encrypted data is discreetly incorporated into an image by altering pixel values at the lowest level without causing any visual change

FUNCTIONAL FLOW OF LASAGNIA



Step 1: Attach an image ,Input Message and input a key

Step 2: Binary Transformation
The message is converted into a sequence of binary bits (0s and 1s).

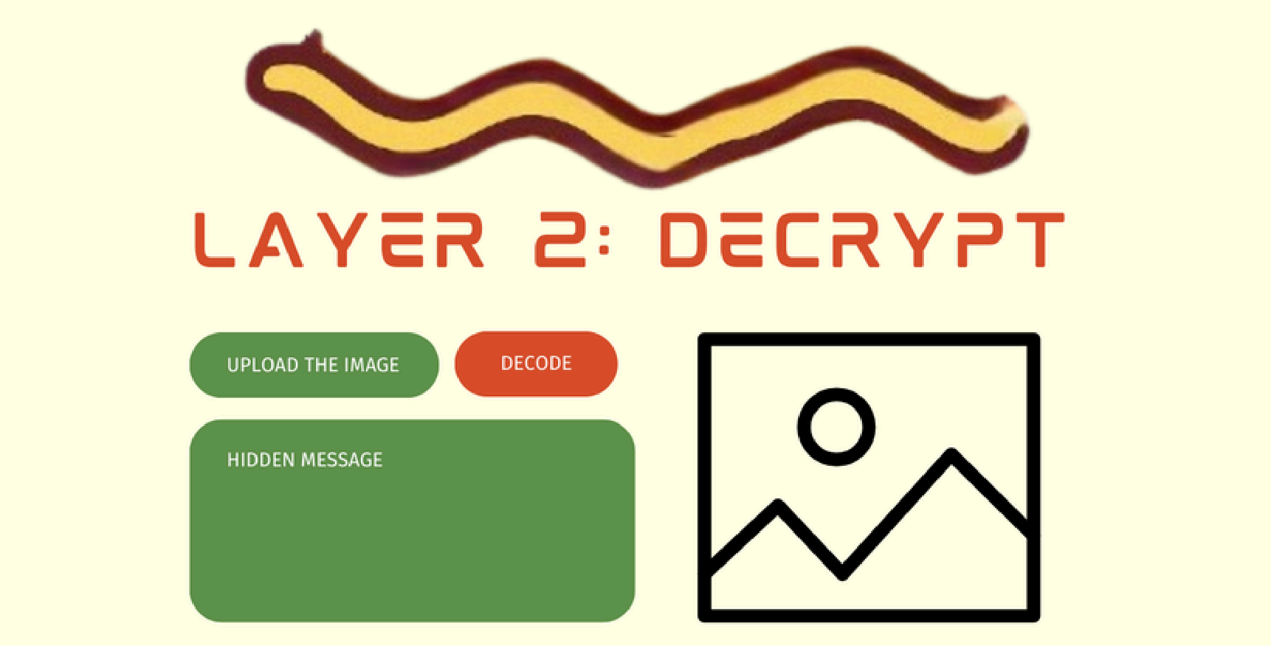
Step 3: Obfuscation
Every 8 real bits, Lasagna inserts 1 fake random bit 0 or 1.

- Example:
  - Original: 01001101
  - Obfuscated: 01001101 + 1 (fake) → 01001101 1
  -

Step 4: Encryption with XOR
Each bit of the binary message is encrypted by applying the XOR logical operation with a secret key.
Formula: Ciphertext Bit=Plaintext Bit⊕Key Bit

Step 5: Steganographic Embedding
The encrypted bits are hidden inside the Least Significant Bits (LSBs) of the image's pixel values. This modification is subtle and does not visibly alter the image.

Step 6: Saving the Stego-Image
The modified image (now containing the encrypted secret) is saved. Visually, it looks identical to the original, unmodified image.



Decoding and Retrieving the Secret Message:

Step 7: Load the Stego-Image

The stego-image is loaded into Lasagnia for message extraction.

Step 8: Extract Hidden Data

The tool reads the Least Significant Bits (LSBs) of the image's pixels to retrieve the embedded encrypted binary data.

Step 9: Decryption with XOR

The extracted binary data is decrypted by applying the XOR operation again with the same secret key used during encryption.

Formula: Plaintext Bit=Ciphertext Bit⊕Key Bit

Step 10: Binary to Text Conversion

The decrypted binary sequence is converted back into readable text, reconstructing the original secret message.

THEORETICAL ASPECTS

Obfuscation: Game-Theoretic Defense

Lasagnia intentionally inserts decoy bits into the encrypted message to further confuse attackers and add plausible deniability.

XOR Cipher: Mathematical Basis

Lasagna encrypts messages using the XOR operation, where each bit of the plaintext is combined with a key bit. The method is fast and secure if the key is random and secret.

Bitwise XOR operation between plaintext (P) and key (K):

- $C=P\oplus KC=P\oplus K$
- $P=C\oplus KP=C\oplus K$

Steganography: Invisible Embedding

After encryption, the message is hidden inside an image using Least Significant Bit (LSB) steganography. Only the least important pixel bits are altered, leaving the image visually unchanged.

Security Principle: Kerckhoffs's Law

Lasagna follows Kerckhoffs's Principle:

Security must rely on the secrecy of the key, not on the secrecy of the system. Even if the technique is known, without the key, the hidden message remains protected.

STRENGTHS

✅ Multiple-layer protection: Encryption + Stealth hiding +Obfuscation
✅ No detectable transmission: Looks like an ordinary image
✅ Privacy by design: Data never leaves the user's device
✅ User independence: No need for third-party tools or servers
✅ Simple interface: Accessible to non-experts

LIMITATIONS

⚠ XOR is simple: Security depends on key strength and randomness
→ Fix: Use a long, random key.
⚠ Larger messages require larger carrier files
→ Fix: Use high-resolution pictures

CONCLUSION

LASAGNA offers a simple yet highly effective approach to modern data protection.
By integrating encryption, steganography, and obfuscation, it ensures that secrets are secured, hidden, and protected against both casual and advanced threats.
Its lightweight, user-centered design makes it accessible without compromising on security.