Implementation and Cryptanalysis of a Simplified AES-like Cipher

Japan Group
Information Security Lab, 2024/2025

A. Rotondo, S. Pietrogrande, S. Masiero, A. Mutti

Introduction

This report describes our work on the implementation and cryptanalysis of a simplified AES-like cipher as presented in the laboratory session. The cipher is an iterated scheme with $n = 5$ rounds over the finite field $\mathbb{F}_{11}$, processing 8-symbol blocks. For key management, a main key is used to derive six subkeys (each of length 4) by a linear transformation. In addition to the linear variant, we implemented a nearly linear version (using a substitution lookup table) and a non-linear variant (using the multiplicative inverse in $\mathbb{F}_{11}$). In the following sections we briefly describe our implementation for Tasks 1–8 and report the results of our cryptanalysis.

Implementation Overview and Task Descriptions

Task 1 & 2: Encryption and Decryption

We implemented the encryption function by processing the plaintext block through five rounds. Each round performs:

- a subkey addition (adding the subkey twice to the block, modulo 11),
- a substitution step ($f(v) = 2v \mod 11$ for the linear variant),
- a transposition (flipping the second half of the vector),
- and a linear transformation (writing the transposed vector into a 2×4 matrix, multiplying by a fixed matrix, and reading the result row-wise).

The linear transformation is not performed on the last cycle as described in the scheme.

The decryption function applies the inverse operations in reverse order. We verified the correctness by checking that encrypting $u = [1, 0, \ldots, 0]$ with $k = [1, 0, \ldots, 0]$ produces $x = [4, 0, 0, 9, 7, 0, 0, 3]$, and that decryption recovers the original plaintext.

Task 3 & 4: Linear Cryptanalysis

We observed that both the substitution function and the subkey generation are linear; hence, the cipher is linear. We identified matrices $A \in \mathbb{F}_{11}^{8\times 8}$ and $B \in \mathbb{F}_{11}^{8\times 8}$ such that

$$x = E(k, u) = A\,k + B\,u \mod 11.$$

These matrices were computed by encrypting the standard basis vectors for the key and the plaintext (see Appendix 1 in the instructions). Using a known plaintext-ciphertext pair, we recovered the key with

$$k = A^{-1}(x - B\,u) \mod 11.$$

Our experiments yielded, for example, the candidate

$$\hat{k} = [6, 6, 5, 4, 6, 5, 2, 8].$$

Task 5 & 6: Nearly Linear Variant and Its Cryptanalysis

For the nearly linear cipher, the substitution function is defined via the following table:

$v_i(j)$	0	1	2	3	4	5	6	7	8	9	10
$y_i(j)$	0	2	4	8	6	10	1	3	5	7	9

We implemented this by replacing the linear substitution with a lookup table. To perform cryptanalysis, we computed an approximate linear relation using matrices A, B, and an additional matrix C (possibly $C = I$). We then estimated the probability

$$\mathbb{P}[A\,k + B\,u + C\,x = 0] \gg \frac{1}{11^8},$$

via numerical simulation. Based on these matrices, we recovered a candidate key from the nearly linear KPA data.

Our estimated probability was approximately $2 \cdot 10^{-5}$ with the threshold $4.665073802 \cdot 10^{-9}$.

We were able to recover the key through a brute-force approach due to the simplicity of the encryption mechanism. The cipher's inherent linearity, particularly in the substitution and subkey generation functions, results in a relatively small and structured key space. This allowed us to efficiently test all possible key candidates until we identified the correct key.

$$\hat{k} = [7, 6, 3, 9, 0, 9, 2, 9].$$

Task 7 & 8: Non-Linear Cipher and Meet-in-the-Middle Attack

For the non-linear variant, the substitution is modified to use the multiplicative inverse in $\mathbb{F}_{11}$:

$$f(v) = 2\,v^{-1} \mod 11,$$

with appropriate adjustments in the subkey generation (the key length is reduced to 4). To attack the concatenated cipher (where encryption is performed with two different keys k' and k''), we implemented a meet-in-the-middle (MITM) attack. This method involves generating candidate keys for the first and second cipher instances, computing intermediate values, and matching them to recover the pair:

$$\hat{k}' = [0, 5, 4, 0], \quad \hat{k}'' = [10, 8, 0, 6].$$

Results and Conclusion

Our implementation confirmed the expected behavior in each variant. For the linear cipher, the vulnerability was clearly demonstrated by recovering $\hat{k} = [6, 6, 5, 4, 6, 5, 2, 8]$ via matrix inversion. In the nearly linear version, although the substitution is modified, the approximate linearity still permitted successful cryptanalysis with an estimated probability of approximately $0,09058$. The non-linear variant required a more advanced MITM attack, which reduced the search complexity and successfully identified the two key parts.

In summary, our experiments validate the theoretical vulnerabilities of the simplified AES-like cipher in its linear and nearly linear forms and demonstrate that additional non-linearity (combined with a meet-in-the-middle approach) is necessary to thwart such attacks. The complete source code is provided separately.

Matrices and Keys:
Task 3: Matrices A and B (obtained via `findMatrixKey` and `findMatrixMessage`):

$$\text{Mat A} = \begin{bmatrix} 9 & 0 & 1 & 6 & 0 & 0 & 1 & 10 \\ 0 & 8 & 6 & 2 & 2 & 9 & 0 & 0 \\ 0 & 6 & 0 & 8 & 3 & 10 & 0 & 0 \\ 6 & 0 & 0 & 8 & 0 & 1 & 6 & 6 \\ 2 & 0 & 1 & 10 & 0 & 0 & 1 & 3 \\ 0 & 1 & 8 & 4 & 9 & 6 & 0 & 0 \\ 0 & 10 & 0 & 5 & 7 & 6 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 & 1 & 4 & 8 \end{bmatrix} \qquad \text{Mat B} = \begin{bmatrix} 6 & 0 & 0 & 3 & 3 & 0 & 0 & 0 \\ 0 & 6 & 3 & 0 & 0 & 3 & 0 & 0 \\ 0 & 3 & 6 & 0 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 6 & 0 & 0 & 0 & 3 \\ 5 & 0 & 0 & 0 & 4 & 0 & 0 & 8 \\ 0 & 5 & 0 & 0 & 0 & 4 & 8 & 0 \\ 0 & 0 & 5 & 0 & 0 & 8 & 4 & 0 \\ 0 & 0 & 0 & 5 & 8 & 0 & 0 & 4 \end{bmatrix}$$

Task 4: Recovered key: $\hat{k} = [6, 6, 5, 4, 6, 5, 2, 8]$.

Task 5: Matrices A, B, and C for the nearly linear variant and estimated probability $P[A\,k + B\,u + C\,x = 0] \approx 2 \cdot 10^5$.

$$\text{Mat A} = \begin{bmatrix} 9 & 0 & 1 & 6 & 0 & 0 & 1 & 10 \\ 0 & 8 & 6 & 2 & 2 & 9 & 0 & 0 \\ 0 & 6 & 0 & 8 & 3 & 10 & 0 & 0 \\ 6 & 0 & 0 & 8 & 0 & 1 & 6 & 6 \\ 2 & 0 & 1 & 10 & 0 & 0 & 1 & 3 \\ 0 & 1 & 8 & 4 & 9 & 6 & 0 & 0 \\ 0 & 10 & 0 & 5 & 7 & 6 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 & 1 & 4 & 8 \end{bmatrix} \qquad \text{Mat B} = \begin{bmatrix} 9 & 0 & 0 & 2 & 6 & 0 & 0 & 2 \\ 0 & 9 & 2 & 0 & 0 & 6 & 2 & 0 \\ 0 & 2 & 9 & 0 & 0 & 2 & 6 & 0 \\ 2 & 0 & 0 & 9 & 2 & 0 & 0 & 6 \\ 9 & 0 & 0 & 5 & 2 & 0 & 0 & 2 \\ 0 & 9 & 5 & 0 & 0 & 2 & 2 & 0 \\ 0 & 5 & 9 & 0 & 0 & 2 & 2 & 0 \\ 5 & 0 & 0 & 9 & 2 & 0 & 0 & 2 \end{bmatrix}$$

$$\text{Mat C} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

Task 6: Recovered key for nearly linear cipher: $\hat{k} = [7, 6, 3, 9, 0, 9, 2, 9]$.

Task 8: Recovered non-linear keys: $\hat{k}' = [0, 5, 4, 0]$, $\hat{k}'' = [10, 8, 0, 6]$.