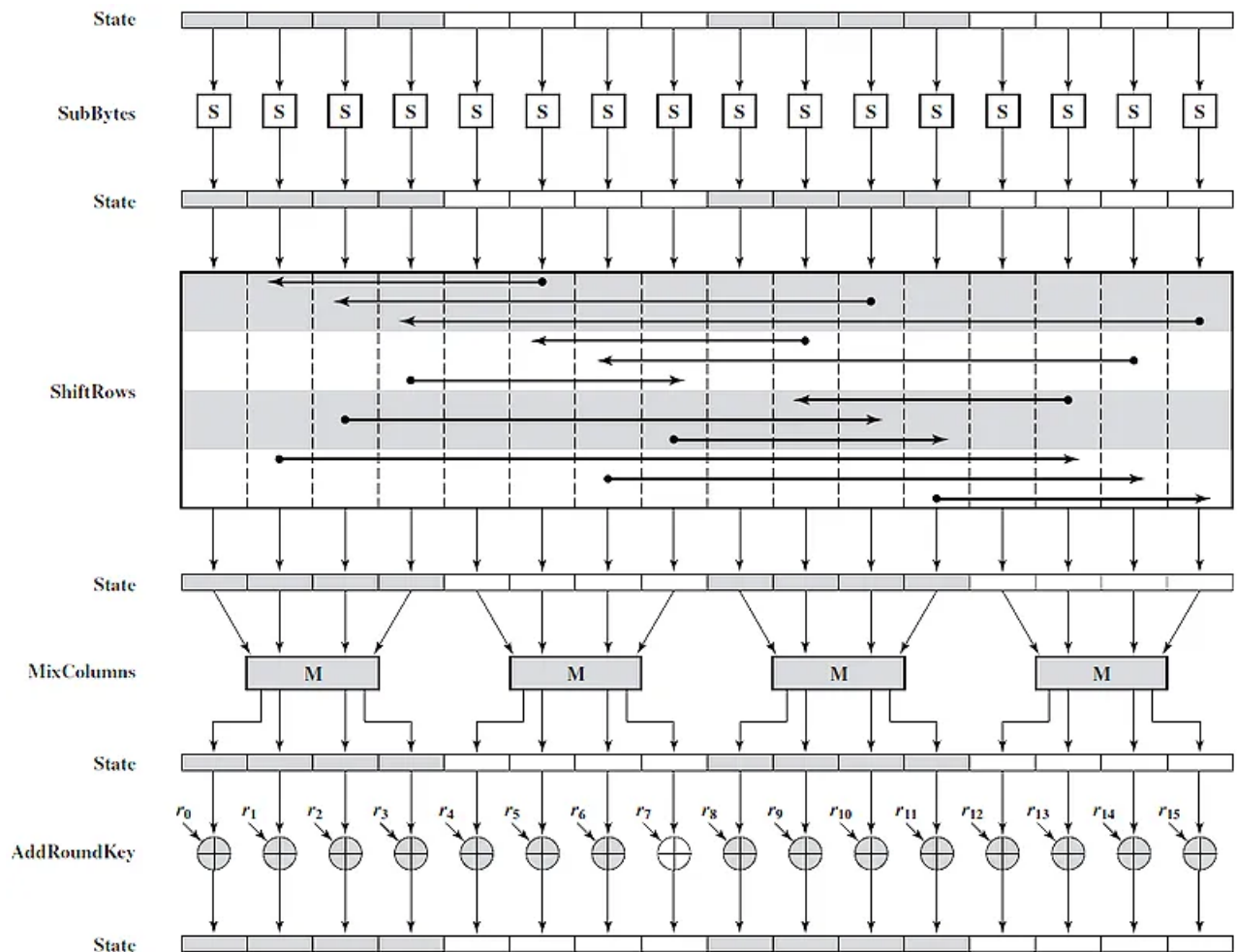


C | SecureAES

- High-Performance AES Encryption in C -

Ji Yong-Hyeon



Department of Information Security, Cryptology, and Mathematics
College of Science and Technology
Kookmin University

October 16, 2024

Acknowledgements

Note (XOR Operation and Modular Reduction in $GF(2^n)$). In the context of Galois Field $GF(2^n)$, particularly in binary polynomial arithmetic, the XOR operation is equivalent to addition and also plays a crucial role in modular reduction. We explore this equivalence through the principles of field theory and polynomial arithmetic.

- **Field Properties:**

A Galois Field, $GF(p^n)$, is a finite field that contains a finite number of elements, where

- p is a prime number (base of the field) and
- n is a positive integer (degree of the field).

For the binary field $GF(2^n)$, $p = 2$, which implies that every element in this field is either 0 or 1.

- **Addition in $GF(2^n)$:**

In $GF(2^n)$, the addition of two elements is performed modulo 2. For any two elements $a, b \in GF(2^n)$, the addition is defined as:

$$a + b = a \oplus b$$

Since 2 is the base of the field, the addition wraps around upon reaching 2, which is effectively what the XOR operation does.

- **Polynomial Representation:**

Elements in $GF(2^n)$ can be represented as polynomials where each coefficient is in $GF(2) = \{0, 1\}$. A general element can be written as:

$$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$$

where $a_i \in \{0, 1\}$ for all i .

- **Modular Reduction:**

Modular reduction in $GF(2^n)$ involves reducing a polynomial by a fixed irreducible polynomial of degree n , ensuring that the result remains within the field. Let $m(x)$ be the irreducible polynomial. The reduction of a polynomial $f(x)$ is given by: $f(x) \bmod m(x)$

- **XOR as Modular Reduction:**

During modular reduction, the subtraction used in polynomial division becomes XOR, because subtraction and addition are the same in $GF(2)$. Therefore, reducing a polynomial $f(x)$ by $m(x)$ is effectively performed using XOR on the coefficients of corresponding terms.

For example, if $f(x)$ has a term x^k where $k \geq n$, and $m(x)$ has a term x^k , then reducing $f(x)$ by $m(x)$ involves XORing the coefficients of x^k in $f(x)$ and $m(x)$, effectively eliminating the x^k term in $f(x)$.

In summary, the XOR operation becomes equivalent to both addition and modular reduction in $GF(2^n)$ due to the binary nature of the field. This equivalence simplifies polynomial arithmetic in binary fields, making it a cornerstone of operations in cryptographic algorithms.

Contents

1	Block Cipher	1
1.1	Definition and Structure	1
1.2	Modes of Operations	2
1.2.1	Padding	2
1.2.2	ECB (Electronic CodeBook)	3
1.2.3	CBC (Cipher Block Chaining)	4
1.2.4	OFB (Output FeedBack)	5
1.2.5	CFB (Ciphertext FeedBack)	5
1.2.6	CTR (CounTeR)	5
1.2.7	CBC – CS (Ciphertext Stealing)	6
2	AES Algorithm	7
2.1	S-Box ($GF(2^8)$)	7
2.2	MixColumns ($GF(2^8)[x]/\langle x^4 + 1 \rangle$)	10
2.3	Little and Big Endian	14
2.3.1	Introduction	14
2.3.2	Marco	15
3	AES-128	18
3.1	Overview of AES-128	18
3.2	Functions and Constants used in AES	19
3.2.1	Key Expansion	19
3.2.2	AddRoundKey	21
3.2.3	SubBytes / InvSubBytes	22
3.2.4	ShiftRows / InvShiftRows	23
3.2.5	MixColumns / InvMixColumns	25
4	AES - 128 / 192 / 256 (Byte Version)	30
4.1	Specification	30
4.2	Key Expansion (General Version)	32
4.3	8-bit AES - 128 / 192 / 256	34
5	Pre-Computation using SubMix	36
5.1	SubMix and InvSubInvMix	36
5.2	8×32 Table Look Up	37
5.3	Generation of 8×32 Tables	38
5.4	Implementation of SubMix and InvSubInvMix	40
6	32-bit AES	41
A	Additional Data A	43

A.1 Substitution-BOX	43
--------------------------------	----

Chapter 1

Block Cipher

Block ciphers are a fundamental component in cryptographic systems. They transform fixed-size blocks of plaintext into ciphertext using a symmetric key. The transformation is designed to be reversible only with knowledge of the key.

1.1 Definition and Structure

- **Secure Pseudo-Random Permutation (PRP) and Substitution Groups:**
 - **Definition:** A block cipher is considered a secure PRP if it is indistinguishable from a random permutation of the input bits, making it resistant to cryptanalysis.
 - **Substitution Groups:** Block ciphers often use substitution-permutation networks (SPNs) that include substitution groups. These groups perform non-linear transformations, crucial for creating cryptographic strength.
- **Confidentiality for Fixed n-bit Data (Blocks):**
 - **Fixed Block Size:** Block ciphers encrypt and decrypt data in fixed-size blocks (commonly 64 or 128 bits). This fixed size is crucial for the algorithm's structure and security.
 - **Padding Schemes:** When the data doesn't fit perfectly into a block, padding schemes are used to fill the remaining space, ensuring consistent block sizes.
- **Block Cipher Operation Modes for Variable-Length Data:**
 - **Mode of Operation:** To handle variable-length data, block ciphers use different modes of operation like CBC (Cipher Block Chaining), CFB (Cipher Feedback), and GCM (Galois/Counter Mode).
 - **Ensuring Security:** Each mode offers distinct features for security and efficiency, often enhancing the cipher's resistance to various attack vectors.
- **Advantages Over Asymmetric Key Cryptography:**
 - **High-Speed Computation:** Block ciphers are generally faster and require less computational power compared to asymmetric key cryptography.
 - **Suitability:** This makes them suitable for encrypting large volumes of data and in environments with limited resources.

- **Deriving Other Cryptographic Functions:**

- **Versatility:** Block ciphers can be used to design other cryptographic functions like hash functions, message authentication codes (MACs), and random number generators.
- **Construction Techniques:** Techniques like Cipher Block Chaining-MAC (CBC-MAC) and Counter mode (CTR) are examples of how block ciphers can be adapted for these purposes.

Block ciphers are a critical element in the cryptographic landscape, providing a versatile and efficient means for securing digital data. Their adaptability and robustness make them an indispensable tool in the design of secure communication protocols and cryptographic systems.

1.2 Modes of Operations

Table 1.1: Comparison of Modes

Mode	Integrity	Authentication	EncryptBlk	DecryptBlk	Padding	IV	$ P \stackrel{?}{=} C $
ECB	○	×	○	○	○	×	$ P < C $
CBC	○	×	○	○	○	○	$ P < C $
OFB	○	×	○	×	×	○	$ P = C $
CFB	○	×	○	×	×	○	$ P = C $
CTR	○	×	○	×	×	○	$ P = C $
CBC – CS	○	×	○	○	×	○	$ P = C $

1.2.1 Padding

Block ciphers require input lengths to be a multiple of the block size. Padding is used to extend the last block of plaintext to the required length. Without proper padding, the encryption process may be insecure or infeasible.

There are several padding schemes used in practice, such as:

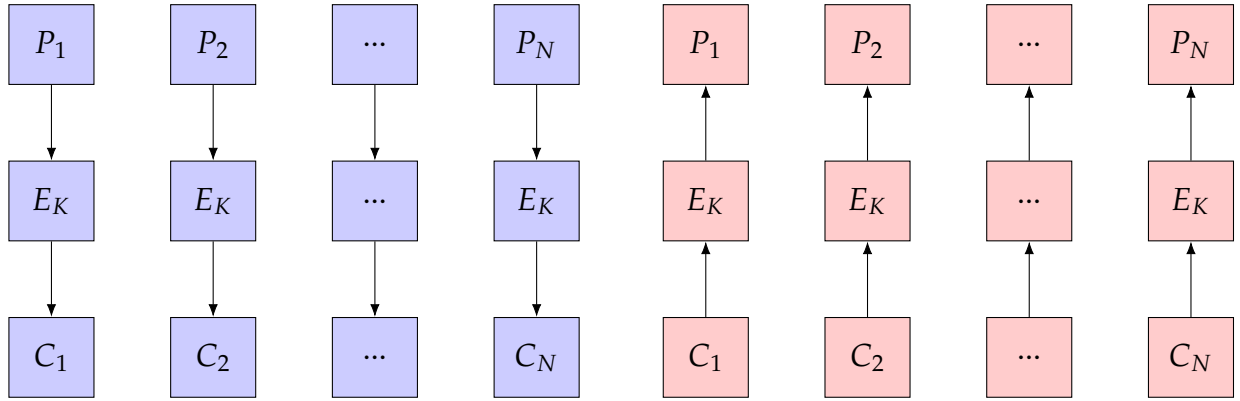
Table 1.2: Padding Standards in Block Ciphers

Standard Name	Padding Method
PKCS#7	Pad with bytes all the same value as the number of padding bytes ...dd dd dd dd dd dd dd dd dd dd dd dd 04 04 04 04
ANSI X9.23	Pad with zeros, last byte is the number of padding bytes ...dd dd dd dd dd dd dd dd dd dd dd dd 00 00 00 00 05
ISO/IEC 7816-4	First byte is '80' (hex), followed by zeros ...dd dd dd dd dd dd dd dd dd dd dd dd 80 00 00 00 00 00
ISO 10126	Pad with random bytes, last byte is the number of padding bytes ...dd dd dd dd dd dd dd dd dd dd dd dd 2e 49 1b c1 aa 06

1.2.2 ECB (Electronic CodeBook)

Algorithm 1: Electronic CodeBook

Input: K and $P = P_1 \parallel \dots \parallel P_N$ ($P_i \in \{0, 1\}^n$) Output: $C = C_1 \parallel \dots \parallel C_N$ ($C_i \in \{0, 1\}^n$)	Input: K and $C = C_1 \parallel \dots \parallel C_N$ ($C_i \in \{0, 1\}^n$) Output: $P = P_1 \parallel \dots \parallel P_N$ ($P_i \in \{0, 1\}^n$)
<pre> 1 for $i \leftarrow 1$ to N do 2 $C_i \leftarrow \text{EncryptBlk}(K, P_i);$ 3 end 4 return $C = C_1 \parallel \dots \parallel C_N;$ </pre>	<pre> 1 for $i \leftarrow 1$ to N do 2 $P_i \leftarrow \text{DecryptBlk}(K, C_i);$ 3 end 4 return $P = P_1 \parallel \dots \parallel P_N;$ </pre>


Remark 1.1.

(1) For a pair of plaintext/ciphertext (P, C) and (P', C') ,

$$P = P' \implies C = C'.$$

- (2) A single-bit error in the ciphertext affects only the corresponding block in the decryption.
- (3) Block order changes, as well as additions/deletions, are possible. Therefore, to ensure the integrity of the ciphertext (i.e., detection or prevention of tampering), it should be used in conjunction with a checksum or a Message Authentication Code (MAC).

1.2.3 CBC (Cipher Block Chaining)

Algorithm 2: Cipher Block Chaining

Input: K, IV and $P = P_1 \parallel \dots \parallel P_N$
Output: $C = C_1 \parallel \dots \parallel C_N$

```

1  $C_0 \leftarrow IV$ ;
2 for  $i \leftarrow 1$  to  $N$  do
3    $C_i \leftarrow \text{EncryptBlk}(K, P_i \oplus C_{i-1})$ ;
4 end
5 return  $C = C_1 \parallel \dots \parallel C_N$ ;

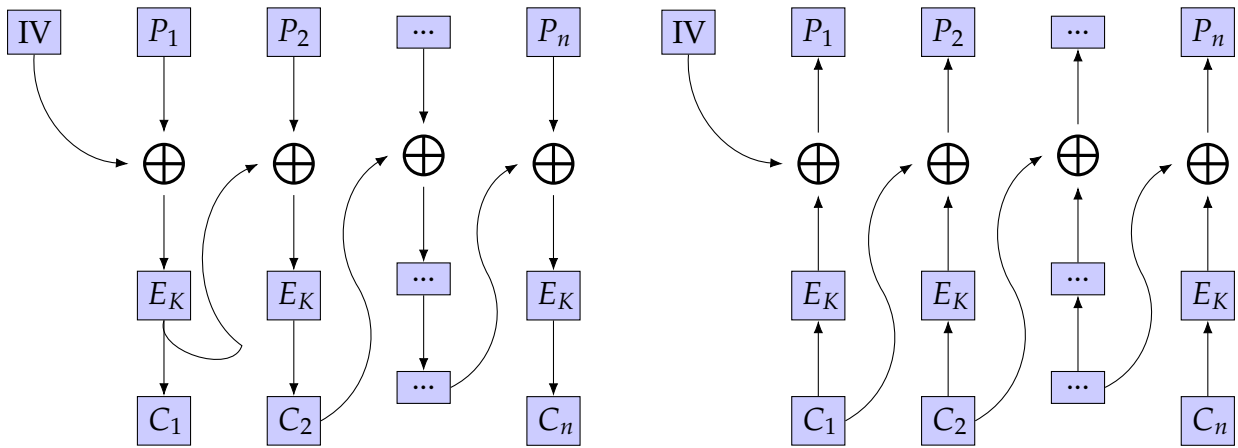
```

Input: K, IV and $C = C_1 \parallel \dots \parallel C_N$
Output: $P = P_1 \parallel \dots \parallel P_N$

```

1  $C_0 \leftarrow IV$ ;
2 for  $i \leftarrow 1$  to  $N$  do
3    $P_i \leftarrow C_{i-1} \oplus \text{DecryptBlk}(K, C_i)$ ;
4 end
5 return  $P = P_1 \parallel \dots \parallel P_N$ ;

```


Remark 1.2.

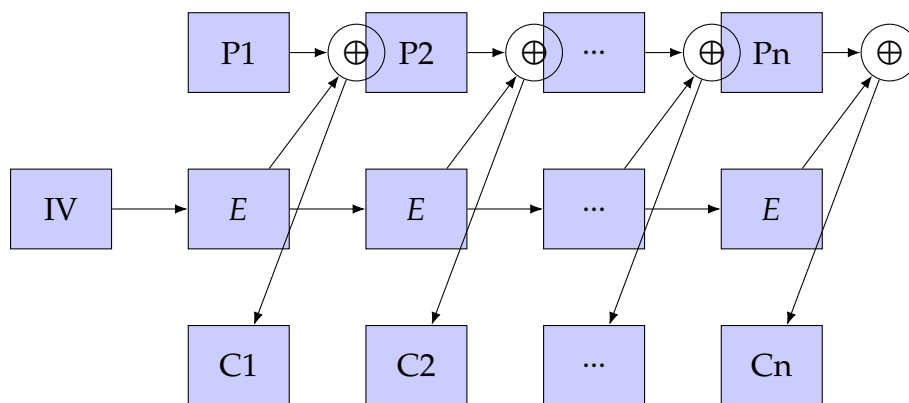
(1) For a set of plaintext/ciphertext pairs (IV, P, C) and (IV', P', C') ,

$$IV = IV' \wedge P = P' \implies C = C'.$$

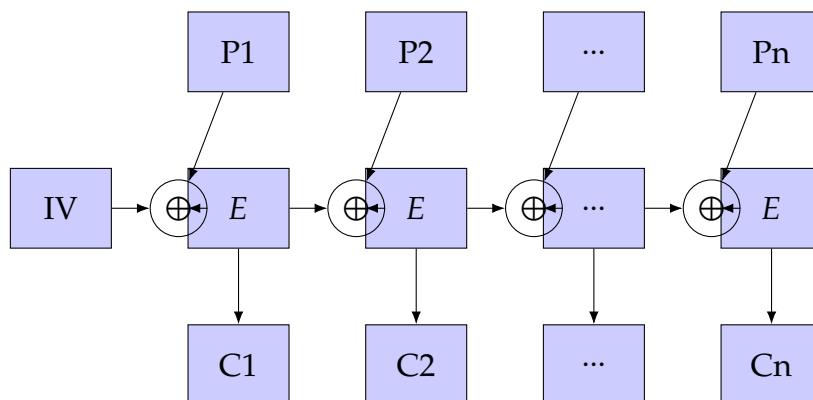
(2) A one-bit error in the ciphertext will affect the corresponding block and the subsequent block in the decryption process, thereby enabling the detection of such errors.

(3) Altering the order of blocks, as well as adding or deleting them, is not possible.

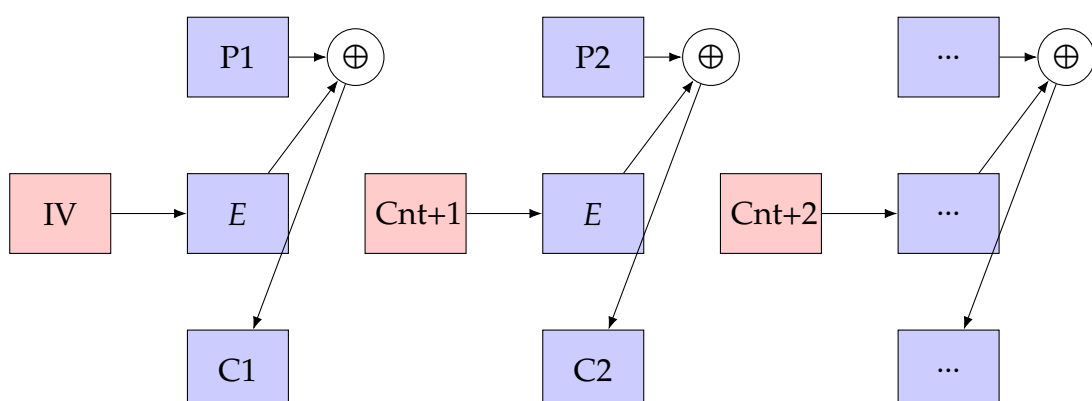
1.2.4 OFB (Output FeedBack)

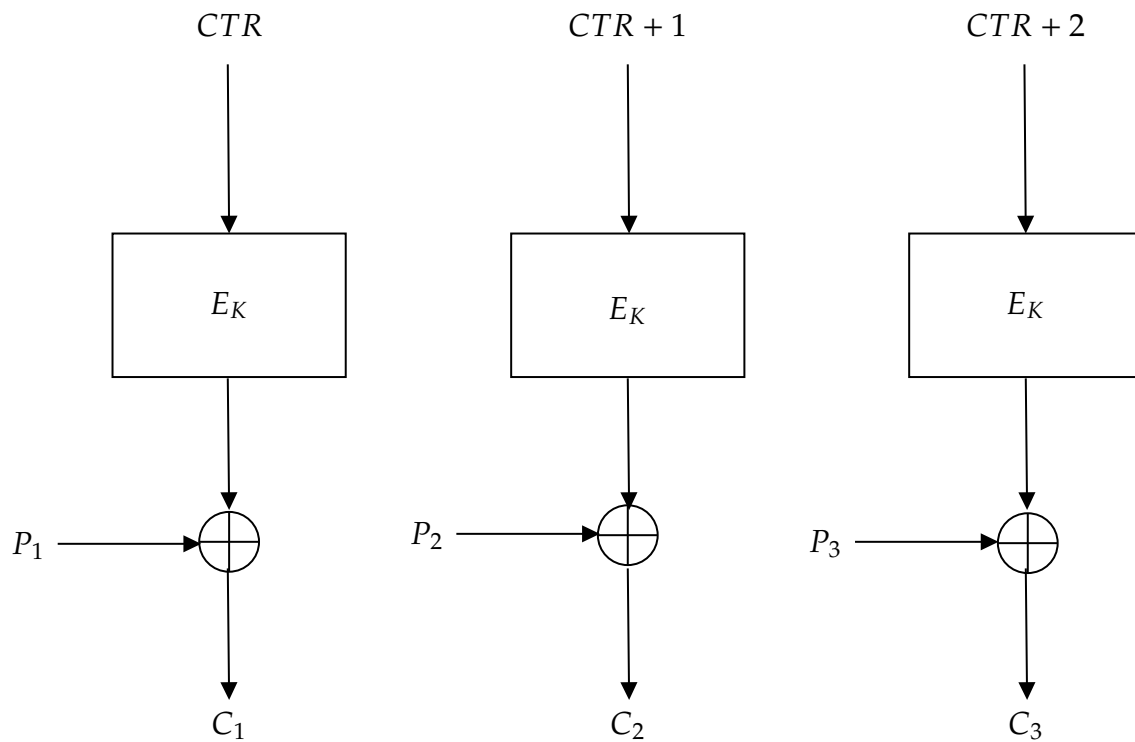


1.2.5 CFB (Ciphertext FeedBack)

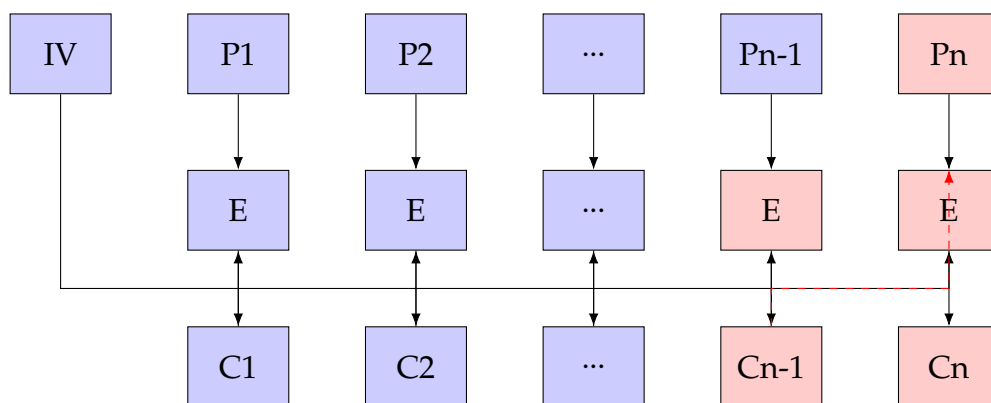


1.2.6 CTR (CounTeR)





1.2.7 CBC – CS (Ciphertext Stealing)



Chapter 2

AES Algorithm

2.1 S-Box ($GF(2^8)$)

Let $m(x) := x^8 + x^4 + x^3 + x + 1$.

$$\begin{aligned} GF(2^8) &= GF(2)[x]/\langle x^8 + x^4 + x^3 + x + 1 \rangle \\ &= GF(2)[x]/\langle m(x) \rangle \\ &= \left\{ b_0 + b_1x + \cdots + b_6x^6 + b_7x^7 : b_0, b_1, \dots, b_6, b_7 \in GF(2) \right\} \\ &= \left\{ \sum_{i=0}^7 b_i x^i : b_i \in \{0, 1\} \right\}. \end{aligned}$$

Let $f(x), g(x) \in GF(2^8)$, say,

$$f(x) = \sum_{i=0}^7 a_i x^i + \langle m(x) \rangle, \quad g(x) = \sum_{j=0}^7 b_j x^j + \langle m(x) \rangle.$$

Then

$$f(x) + g(x) = \sum_{i=0}^7 (a_i + b_i) x^i + \langle m(x) \rangle = \sum_{i=0}^7 (a_i \oplus b_i) x^i + \langle m(x) \rangle.$$

Here, $\oplus : GF(2) \times GF(2) \rightarrow GF(2)$. And

$$f(x) \cdot g(x) = m(x) \cdot q(x) + r(x).$$

Here $\deg r \leq 7$.

We define

$$\begin{aligned} \text{xtime} &: GF(2^8) \longrightarrow GF(2^8) \\ f(x) &\longmapsto x \cdot f(x) \end{aligned}$$

Then

$$1. f(x) = a_0 + a_1x + \cdots + a_6x^6 + a_7x^7$$

2.

$$\begin{aligned} x \cdot f(x) &= a_0x + a_1x^2 + \cdots + a_6x^7 + a_7x^8 \\ &= a_0x + a_1x^2 + \cdots + a_6x^7 + a_7(x^4 + x^3 + x + 1) \quad \because x^8 \equiv x^4 + x^3 + x + 1 \pmod{m(x)} \\ &= \begin{cases} \sum_{i=0}^6 a_i x^{i+1} + 0 & : a_7 = 0 \\ \sum_{i=0}^6 a_i x^{i+1} + (x^4 + x^3 + x + 1) & : a_7 = 1 \end{cases} \\ &= \begin{cases} (f(x) \ll 1) & : a_7 = 0 \\ (f(x) \ll 1) \oplus 0x1b & : a_7 = 1 \end{cases} \end{aligned}$$

```
1  u8 GF256_xtime(u8 f) {
2      return (f & 0x80) ? (f << 1) ^ 0x1b : f << 1;
3  }
```

$$\begin{aligned} g(x) \cdot f(x) &= \sum_{i=0}^7 g(x)a_i x^i \\ &= g(x)a_0 + \sum_{i=1}^7 g(x)a_i x^i \\ &= g(x)a_0 + \textcolor{red}{x} \sum_{i=1}^7 g(x)a_i x^{i-1} \\ &= g(x)a_0 + \textcolor{red}{x} \left(g(x)a_1 + \sum_{i=2}^7 g(x)a_i x^{i-2} \right) \\ &= g(x)a_0 + \textcolor{red}{x} \left(g(x)a_1 + \textcolor{red}{x} \left(g(x)a_2 + \sum_{i=3}^7 g(x)a_i x^{i-3} \right) \right) \\ &= \dots \\ &= g(x)a_0 + \textcolor{red}{x}(g(x)a_1 + \textcolor{red}{x}(g(x)a_2 + \textcolor{red}{x}(g(x)a_3 + \textcolor{red}{x}(g(x)a_4 + \textcolor{red}{x}(g(x)a_5 + \textcolor{red}{x}(g(x)a_6 + \textcolor{red}{x}(g(x)a_7)))))))) \end{aligned}$$

That is,

x	$\cdot 0$	$+(g(x) \cdot a_7)$
x	$\cdot (g(x) \cdot a_7)$	$+(g(x) \cdot a_6)$
x	$\cdot (x \cdot (g(x) \cdot a_7) + (g(x) \cdot a_6))$	$+(g(x) \cdot a_5)$

Step 1. $x \cdot 0 + g(x) \cdot a_7$

Step 2. $x \cdot (g(x) \cdot a_7) + (g(x) \cdot a_6)$

Step 3. $x \cdot (x \cdot (g(x) \cdot a_7) + (g(x) \cdot a_6)) + (g(x) \cdot a_5)$

...

Final. $g \cdot a_0 + x(g \cdot a_1 + \dots + x(g \cdot a_5 + x(g \cdot a_6 + x(g \cdot a_7))))$

```

1  u8 GF256_mul(u8 f, u8 g) {
2      u8 h = 0x00; // h = f * g
3      u8 coef;
4
5      for (i8 i = 7; i >= 0; i--) {
6          coef = (f >> i) & 0x01; // Get the coefficient f_i
7          h = GF256_xtime(h);      // Multiply h by x
8          if (coef == 1) h ^= g;   // If f_i = 1, add g(x) to h(x)
9      }
10
11     return h;
12 }

```

```

1  u8 GF256_MUL(u8 f, u8 g) {
2      u8 h = 0;
3      for (i8 i = 0; i < 8; i++) {
4          h ^= (g & 1) * f;
5          g >>= 1; // g = g / 2.
6
7          u8 msb = f & 0x80;
8          f <<= 1; // f = f * 2.
9          // Conditional XOR without branching.
10         f ^= (0 - ((f & 0x80) >> 7)) & 0x1b; // (f & 0x80) is the
            msb
11     }
12
13     return h;
14 }

```

2.2 MixColumns ($GF(2^8)[x]/\langle x^4 + 1 \rangle$)

$$\text{MixColumns} : \begin{cases} \{\mathbf{0}, \mathbf{1}\}^{128} \longrightarrow \{\mathbf{0}, \mathbf{1}\}^{128} \\ \sum_{i=0}^{127} a_i x^i \longmapsto \sum_{j=0}^{127} b_j x^j \end{cases}$$

X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}
-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	----------	----------	----------	----------	----------	----------

\Downarrow

X'_0	X'_1	X'_2	X'_3	X'_4	X'_5	X'_6	X'_7	X'_8	X'_9	X'_{10}	X'_{11}	X'_{12}	X'_{13}	X'_{14}	X'_{15}
--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	-----------	-----------	-----------	-----------	-----------	-----------

X_0	X_4	X_8	X_{12}
X_1	X_5	X_9	X_{13}
X_2	X_6	X_{10}	X_{14}
X_3	X_7	X_{11}	X_{15}

\Rightarrow

X'_0	X'_4	X'_8	X'_{12}
X'_1	X'_5	X'_9	X'_{13}
X'_2	X'_6	X'_{10}	X'_{14}
X'_3	X'_7	X'_{11}	X'_{15}

Consider

$$GF(2^8)[x]/\langle x^4 + 1 \rangle = \left\{ a_0 + a_1x + a_2x^2 + a_3x^3 : a_i \in GF(2^8) \right\}.$$

Note that $x^5 = (x^4 + 1)x + x \equiv x \pmod{\langle x^4 + 1 \rangle}$. We choose

$$a(x) = (0x03) \cdot x^3 + (0x01) \cdot x^2 + (0x01) \cdot x + (0x02) \in GF(2^8)[x]/\langle x^4 + 1 \rangle,$$

where

$$\begin{aligned} 0x01 &= 0b \ 0000 \ 0001 &= 1, \\ 0x02 &= 0b \ 0000 \ 0010 &= x, \\ 0x03 &= 0b \ 0000 \ 0011 &= x + 1. \end{aligned}$$

Let $b(x) = b_0 + b_1x + b_2x^2 + b_3x^3$, $c(x) = c_0 + c_1x + c_2x^2 + c_3x^3$, and let

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} \mapsto \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_0 \cdot b_0 \bmod x^4 + 1 \\ a_1 \cdot b_1 \bmod x^4 + 1 \\ a_2 \cdot b_2 \bmod x^4 + 1 \\ a_3 \cdot b_3 \bmod x^4 + 1 \end{pmatrix}.$$

Then

$$\begin{aligned} a(x) \cdot b(x) &= (a_3 \cdot b_3) x^6 + (a_3 \cdot b_2 + a_2 \cdot b_3) x^5 \\ &\quad + (a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3) x^4 \\ &\quad + (a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3) x^3 \\ &\quad + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) x^2 \\ &\quad + (a_1 \cdot b_0 + a_0 \cdot b_1) x \\ &\quad + (a_0 \cdot b_0) \\ &= (a_3 \cdot b_3) x^2 + (a_3 \cdot b_2 + a_2 \cdot b_3) x \\ &\quad + (a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3) 1 \\ &\quad + (a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3) x^3 \\ &\quad + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) x^2 \\ &\quad + (a_1 \cdot b_0 + a_0 \cdot b_1) x \\ &\quad + (a_0 \cdot b_0) \quad \text{over } GF(2^8)[x]/\langle x^4 + 1 \rangle \\ &= (a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3) x^3 \\ &= (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2 + a_3 \cdot b_3) x^2 \\ &= (a_1 \cdot b_0 + a_0 \cdot b_1 + a_3 \cdot b_2 + a_2 \cdot b_3) x \\ &= (a_0 \cdot b_0 + a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3) \\ &= c(x). \end{aligned}$$

Thus, we have

$$T : [GF(2^8)]^4 \longrightarrow [GF(2^8)]^4$$

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} \mapsto \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_3 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_0 & a_3 & a_2 & a_1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix},$$

where

$$\begin{pmatrix} a_3 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_0 & a_3 & a_2 & a_1 \end{pmatrix} = \begin{pmatrix} \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} \\ \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} \end{pmatrix}.$$

Here, T has $GF\text{-}MUL \times 16$.

Let $a \in \{\mathbf{0}, \mathbf{1}\}^8$. Then

$$\begin{aligned} \mathbf{02} \otimes a &= \mathbf{xtime}(a), \\ \mathbf{03} \otimes a &= (\mathbf{02} \oplus \mathbf{01}) \otimes a \\ &= (\mathbf{02} \otimes a) \oplus (\mathbf{01} \otimes a) \\ &= \mathbf{xtime}(a) \oplus a. \end{aligned}$$

Thus,

$$\begin{aligned} c_0 &= (\mathbf{02} \otimes b_0) \oplus (\mathbf{03} \otimes b_1) \oplus b_2 \oplus b_3 \\ &= \mathbf{xtime}(b_0) \oplus \mathbf{xtime}(b_1) \oplus b_1 \oplus b_2 \oplus b_3 \\ &= \mathbf{xtime}(b_0 \oplus b_1) \oplus b_1 \oplus b_2 \oplus b_3 \quad \because ax + ab = x(a + b) \\ &= \mathbf{temp0} \oplus b_1 \oplus b_2 \oplus b_3. \end{aligned}$$

and so

$$\begin{aligned} c_0 &= (b_0 \oplus b_1 \oplus b_2 \oplus b_3) \oplus \mathbf{temp0} \oplus b_0 && \text{with } \mathbf{temp0} = \mathbf{xtime}(b_0 \oplus b_1), \\ c_1 &= (b_0 \oplus b_1 \oplus b_2 \oplus b_3) \oplus \mathbf{temp1} \oplus b_1 && \text{with } \mathbf{temp1} = \mathbf{xtime}(b_1 \oplus b_2), \\ c_2 &= (b_0 \oplus b_1 \oplus b_2 \oplus b_3) \oplus \mathbf{temp2} \oplus b_2 && \text{with } \mathbf{temp2} = \mathbf{xtime}(b_2 \oplus b_3), \\ c_3 &= (b_0 \oplus b_1 \oplus b_2 \oplus b_3) \oplus \mathbf{temp3} \oplus b_3 && \text{with } \mathbf{temp3} = \mathbf{xtime}(b_3 \oplus b_0). \end{aligned}$$

That is,

```

1 sum ← b0 ⊕ b1 ⊕ b2 ⊕ b3;
2 c0 ← sum ⊕ temp0 ⊕ b0;
3 c1 ← sum ⊕ temp1 ⊕ b1;
4 c2 ← sum ⊕ temp2 ⊕ b2;
5 c3 ← sum ⊕ temp3 ⊕ b3;

```

It has $\mathbf{xtime}() \times 4$.

Consider

$$\begin{aligned} [a(x)]^1 &= a_3x^3 + a_2x^2 + a_1x + a_0, \\ [a(x)]^2 &= (a_3^2 + a_1^2)x^2 + (a_2^2 + a_0^2), \\ [a(x)]^4 &= a_3^4 + a_2^4 + a_1^4 + a_0^4. \end{aligned}$$

Let $a(x) = (\mathbf{03})x^3 + x^2 + x + (\mathbf{02})$. Then

$$\begin{aligned} [a(x)]^2 &= (\mathbf{04})x^2 + (\mathbf{05}), \\ [a(x)]^3 &= (\mathbf{0b})x^3 + (\mathbf{0d})x^2 + (\mathbf{09})x + (\mathbf{0e}), \end{aligned}$$

and so $[a(x)]^{-1} = [a(x)]^3 = (\mathbf{0b})x^3 + (\mathbf{0d})x^2 + (\mathbf{09})x + (\mathbf{0e})$.

2.3 Little and Big Endian

2.3.1 Introduction

```
1 u8 b[4] = { 0x00, 0x01, 0x02, 0x03 };
2 u32 x = 0x00010203;
```

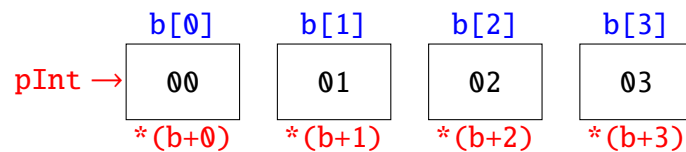
```
>>> x/4xb b
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x/4xb &x
0x7fffffffdd290: 0x03    0x02    0x01    0x00
```

$[u32 \rightarrow (u8 \times 4)] :$

```
b[0] = (x >> 0x18)
b[1] = (x >> 0x10) ^ 0xff
b[2] = (x >> 0x08) ^ 0xff
b[3] = (x          ) ^ 0xff
```

$[(u8 \times 4) \rightarrow u32] :$

```
x = (b[0] << 0x18) ^
     (b[1] << 0x10) ^
     (b[2] << 0x08) ^
     (b[3]          )
```



$b \iff \&(b[0]) \iff (u8*)\&b[0]$

```
1 u8 b[4] = { 0x00, 0x01, 0x02, 0x03 };
2 u32* pInt;
3 u32 x;
4
5 pInt = (u32*)b;
6 x = *pInt;
```

```
>>> x/4xb b
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x/4xb pInt
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x/4xb &x
0x7fffffffdd284: 0x00    0x01    0x02    0x03
>>> print /x x
$1 = 0x3020100
```

$$\text{u8 } b[4] = \{ 0x00, 0x01, 0x02, 0x03 \}; \implies \begin{cases} \text{u32 } x = 0x03020100; \\ \text{u32 } y = 0x00010203; \end{cases}$$

```

1  u8 b[4] = { 0x00, 0x01, 0x02, 0x03 };
2  u32* px = (u32*)b;
3  u32 x, y;
4
5  x = *px;
6  y = ((u32)b[0] << 0x18) ^
7      ((u32)b[1] << 0x10) ^
8      ((u32)b[2] << 0x08) ^
9      ((u32)b[3] );

```

```

>>> x/4xb b
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x/4xb px
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x /4xb &x
0x7fffffffdd280: 0x00    0x01    0x02    0x03
>>> x /4xb &y
0x7fffffffdd284: 0x03    0x02    0x01    0x00
>>> x /wx 0x7fffffffdd280
0x7fffffffdd280: 0x03020100
>>> x /wx 0x7fffffffdd284
0x7fffffffdd284: 0x00010203

```

2.3.2 Marco

```

1  #define GETU32(pt) ((u32)(pt)[0] << 0x18) ^ \
2                      ((u32)(pt)[1] << 0x10) ^ \
3                      ((u32)(pt)[2] << 0x08) ^ \
4                      ((u32)(pt)[3] )
5
6  u8 b[4] = { 0x00, 0x01, 0x02, 0x03 };
7  u32 y;
8
9  y = GETU32(b);

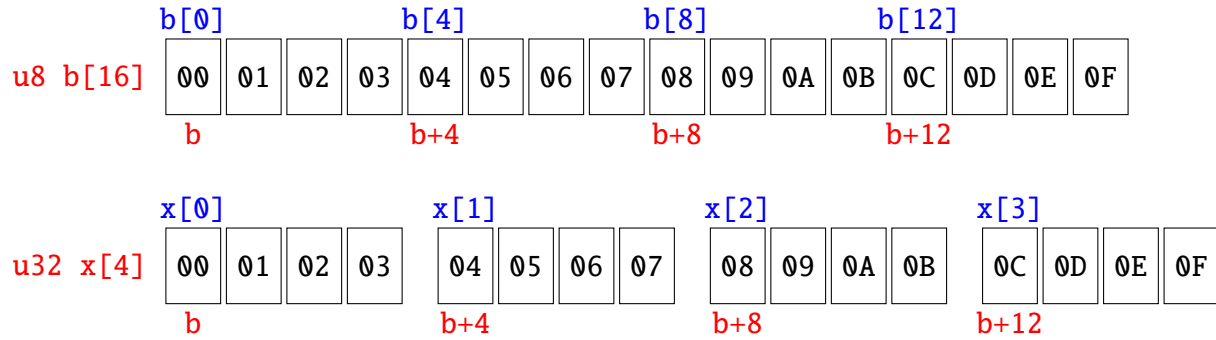
```

```

>>> x/4xb b
0x7fffffffdd294: 0x00    0x01    0x02    0x03
>>> x/4xb &y
0x7fffffffdd290: 0x03    0x02    0x01    0x00

```

Byte to Word



```

1  u8 b[16] = { 0x00, 0x01, 0x02, 0x03,
2                0x04, 0x05, 0x06, 0x07,
3                0x08, 0x09, 0x0A, 0x0B,
4                0x0C, 0x0D, 0x0E, 0x0F};
5
6  u32 x[4] = { GETU32(b          ),
7                GETU32(b + 0x04),
8                GETU32(b + 0x08),
9                GETU32(b + 0x0C)};

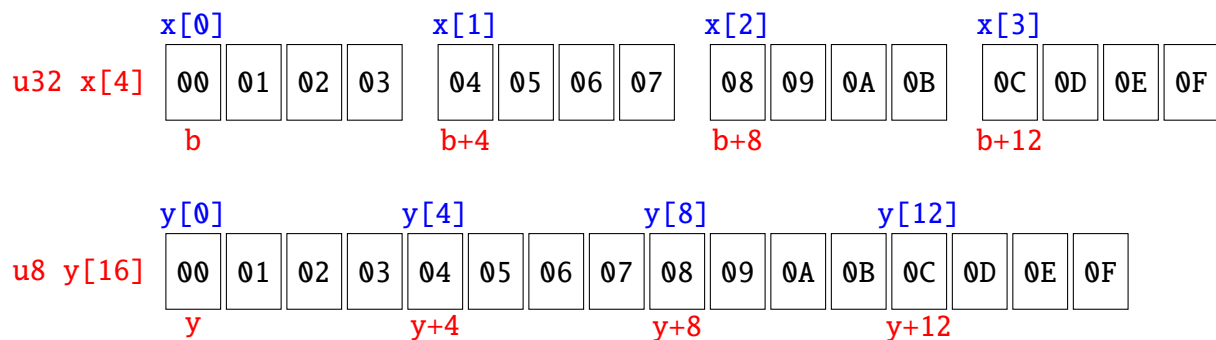
```

```

>>> x/16xb b
0x7fffffffdd280: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
0x7fffffffdd288: 0x08 0x09 0x0a 0x0b 0x0c 0x0d 0x0e 0x0f
>>> x/16xb x
0x7fffffffdd270: 0x03 0x02 0x01 0x00 0x07 0x06 0x05 0x04
0x7fffffffdd278: 0x0b 0x0a 0x09 0x08 0x0f 0x0e 0x0d 0x0c

```

Word to Byte



```

1  #define PUTU32(ct, st) { (ct)[0] = (u8)((st) >> 0x18); \
2                          (ct)[1] = (u8)((st) >> 0x10); \
3                          (ct)[2] = (u8)((st) >> 0x08); \
4                          (ct)[3] = (u8)((st) >> 0x00); }
5
6  u32 x[4] = { 0x00010203, 0x04050607, 0x08090A0B, 0x0C0D0E0F };
7  u8 y[16];
8
9  PUTU32(y, x[0]);
10 PUTU32(y + 0x04, x[1]);
11 PUTU32(y + 0x08, x[2]);
12 PUTU32(y + 0x0C, x[3]);

```

```

>>> x/16xb x
0x7ffffffffffd260: 0x03 0x02 0x01 0x00 0x07 0x06 0x05 0x04
0x7ffffffffffd268: 0x0b 0x0a 0x09 0x08 0x0f 0x0e 0x0d 0x0c
>>> x/16xb y
0x7ffffffffffd280: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
0x7ffffffffffd288: 0x08 0x09 0x0a 0x0b 0x0c 0x0d 0x0e 0x0f

```

Chapter 3

AES-128

3.1 Overview of AES-128

- KeyExpansion : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{1408=4 \cdot (10+1) \cdot 32}$.
- AddRoundKey : $\{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$.
- SubBytes/ShiftRows/MixColumns : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$.

Algorithm 3: Encryption of AES-128

Input: block $\text{src} \in \{0, 1\}^{128}$, round-keys $\{rk_i\}_{i=0}^{11}$ ($rk_i \in \{0, 1\}^{128}$)
Output: block $\text{dst} \in \{0, 1\}^{128}$

```
1  $t \leftarrow \text{AddRoundKey}(\text{src}, rk_0);$ 
2 for  $i \leftarrow 1$  to 9 do
3    $t \leftarrow (\text{MixColumns} \circ \text{ShiftRows} \circ \text{SubBytes})(t);$ 
4    $t \leftarrow \text{AddRoundKey}(t, rk_i);$ 
5 end
6  $t \leftarrow (\text{ShiftRows} \circ \text{SubBytes})(t);$ 
7  $t \leftarrow \text{AddRoundKey}(t, rk_{10});$ 
8  $\text{dst} \leftarrow t;$ 
9 return  $\text{dst};$ 
```

Algorithm 4: Decryption of AES-128

Input: block $\text{src} \in \{0, 1\}^{128}$, round-keys $\{rk_i\}_{i=0}^{11}$ ($rk_i \in \{0, 1\}^{128}$)
Output: block $\text{dst} \in \{0, 1\}^{128}$

```
1  $t \leftarrow \text{AddRoundKey}(\text{src}, rk_{10});$ 
2 for  $i \leftarrow 9$  to 1 do
3    $t \leftarrow (\text{InvSubBytes} \circ \text{InvShiftRows})(t);$ 
4    $t \leftarrow \text{AddRoundKey}(t, rk_i);$ 
5    $t \leftarrow \text{InvMixColumns}(t);$ 
6 end
7  $t \leftarrow (\text{InvShiftRows} \circ \text{InvSubBytes})(t);$ 
8  $t \leftarrow \text{AddRoundKey}(t, rk_0);$ 
9  $\text{dst} \leftarrow t;$ 
10 return  $\text{dst};$ 
```

3.2 Functions and Constants used in AES

3.2.1 Key Expansion

- **RotWord** : $\{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$ is defined by

$$\text{RotWord}(X_0 \parallel X_1 \parallel X_2 \parallel X_3) := X_1 \parallel X_2 \parallel X_3 \parallel X_0 \quad \text{for } X_i \in \{0, 1\}^8.$$

Code 3.1: RotWord rotates the input word left by one byte

```

1 u32 RotWord(u32 word) {
2     return (word << 0x08) | (word >> 0x18);
3 }

```

- **SubWord** : $\{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$ is defined by

$$\text{SubWord}(X_0 \parallel X_1 \parallel X_2 \parallel X_3) := s(X_0) \parallel s(X_1) \parallel s(X_2) \parallel s(X_3) \quad \text{for } X_i \in \{0, 1\}^8.$$

Here, $s : \{0, 1\}^8 \rightarrow \{0, 1\}^8$ is the **S-box**.

Code 3.2: SubWord applies the S-box to each byte of the input word

```

1 u32 SubWord(u32 word) {
2     return (u32)s_box[word >> 0x18] << 0x18 |
3         (u32)s_box[(word >> 0x10) & 0xFF] << 0x10 |
4         (u32)s_box[(word >> 0x08) & 0xFF] << 0x08 |
5         (u32)s_box[word & 0xFF];
6 }

```

- **Round Constant rCon**:

The constant $\text{rCon}_i \in \mathbb{F}_{2^8}$ used in generating the i -th round key corresponds to the value of x^{i-1} in the binary finite field \mathbb{F}_{2^8} and is as follows:

i	1	2	3	4	5	6	7	8	9	10
rCon_i	0x01	0x02	0x04	0x08	0x10	0x20	0x40	0x80	0x1b	0x36

Code 3.3: rCon Array Declaration

```

1 static const u32 rCon[10] = {
2     0x01000000, 0x02000000, 0x04000000, 0x08000000,
3     0x10000000, 0x20000000, 0x40000000, 0x80000000,
4     0x1b000000, 0x36000000
5 };

```

Algorithm 5: Key Schedule (AES-128)

Input: User key $uk = (uk_0, \dots, uk_{15})$ ($uk_i \in \{0, 1\}^8$); // $uk \in \{0, 1\}^{128}$ is 16-byte

Output: round-keys $\{rk_i\}_{i=0}^{43}$ ($rk_i \in \{0, 1\}^{32}$); // $\{rk_i\}_{i=0}^{43} \in \{0, 1\}^{1408}$ is 176-byte

```

1  $rk_0 \leftarrow uk_0 \parallel uk_1 \parallel uk_2 \parallel uk_3$ ;
2  $rk_1 \leftarrow uk_4 \parallel uk_5 \parallel uk_6 \parallel uk_7$ ;
3  $rk_2 \leftarrow uk_8 \parallel uk_9 \parallel uk_{10} \parallel uk_{11}$ ;
4  $rk_3 \leftarrow uk_{12} \parallel uk_{13} \parallel uk_{14} \parallel uk_{15}$ ;
5 for  $i = 4$  to 43 do
6    $t \leftarrow rk_{i-1}$ ;
7   if  $i \bmod 4 = 0$  then
8     /* SubWord  $\circ$  RotWord :  $\{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$  */
9      $t \leftarrow \text{RotWord}(t)$ ;
10     $t \leftarrow \text{SubWord}(t)$ ;
11     $t \leftarrow t \oplus (\text{rCon}_{i/4} \parallel 0x00 \parallel 0x00 \parallel 0x00)$ ;
12  end
13   $rk_i \leftarrow rk_{i-4} \oplus_{32} t$ ;
14 end

```

Code 3.4: AES-128 Key Expansion

```

1 void KeyExpansion(const u8* uKey, u32* rKey) {
2   u32 temp;
3   int i = 0;
4
5   // Copy the input key to the first round key
6   while (i < 4) {
7     rKey[i] = (u32)uKey[4*i] << 0x18 |
8     (u32)uKey[4*i+1] << 0x10 |
9     (u32)uKey[4*i+2] << 0x08 |
10    (u32)uKey[4*i+3];
11    i++;
12  }
13
14  i = 4;
15
16  // Generate the remaining round keys
17  while (i < 44) {
18    temp = rKey[i-1];
19    if (i % 4 == 0) {
20      temp = SubWord(RotWord(temp)) ^ rCon[i/4-1];
21    }
22    rKey[i] = rKey[i-4] ^ temp;
23    i++;
24  }
25 }

```

3.2.2 AddRoundKey

- $\text{AddRoundKey} : \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

$$\text{AddRoundKey} \left(\{X_i\}_{i=0}^{15}, \{rk_i\}_{i=0}^3 \right) := \{X_i \oplus_8 rk_i\}_{i=0}^{15}.$$

Code 3.5: AES AddRoundKey

```

1 void AddRoundKey(u8* state, const u32* rKey) {
2     for (int i = 0; i < AES_BLOCK_SIZE; i++) {
3         // i = 0, 1, 2, 3 => wordIndex = 0
4         // i = 4, 5, 6, 7 => wordIndex = 1
5         // i = 8, 9, 10, 11 => wordIndex = 2
6         // i = 12, 13, 14, 15 => wordIndex = 3
7         int wordIndex = i / 4;
8
9         // i = 0, 1, 2, 3 => bytePosition = 0, 1, 2, 3
10        // i = 4, 5, 6, 7 => bytePosition = 0, 1, 2, 3
11        // i = 8, 9, 10, 11 => bytePosition = 0, 1, 2, 3
12        // i = 12, 13, 14, 15 => bytePosition = 0, 1, 2, 3
13        int bytePosition = i % 4;
14        /*
15         * +-----+-----+-----+-----+
16         * | i      | wordIndex | bytePosition | shiftedWord      |
17         * +-----+-----+-----+-----+
18         * | 0-3    | 0        | 0          | rKey[0] >> 0x18  |
19         * |        |        | 1          | rKey[0] >> 0x10  |
20         * |        |        | 2          | rKey[0] >> 0x08  |
21         * |        |        | 3          | rKey[0]          |
22         * +-----+-----+-----+-----+
23         * | 4-7    | 1        | 0          | rKey[1] >> 24    |
24         * |        |        | 1          | rKey[1] >> 16    |
25         * |        |        | 2          | rKey[1] >> 8     |
26         * |        |        | 3          | rKey[1]          |
27         * +-----+-----+-----+-----+
28         * | ...    | ...      | ...        | ...              |
29         * +-----+-----+-----+-----+
30         * | 15     | 3        | 3          | rKey[3]          |
31         * +-----+-----+-----+-----+
32        */
33        u32 shiftedWord =
34            rKey[wordIndex] >> (8 * (3 - bytePosition));
35
36        u8 keyByte = shiftedWord & 0xFF;
37        state[i] ^= keyByte;
38
39        /* Extract the corresponding byte from the round key word */
40        // state[i] ^= (rKey[i / 4] >> (8 * (3 - (i % 4)))) & 0xFF;
41    }
42 }

```

3.2.3 SubBytes / InvSubBytes

- SubBytes : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

$$\text{SubBytes}(\{X_i\}_{i=0}^{15}) = \{s(X_i)\}_{i=0}^{15}.$$

- InvSubBytes : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

$$\text{SubBytes}(\{X_i\}_{i=0}^{15}) = \{s^{-1}(X_i)\}_{i=0}^{15}.$$

Table 3.1: Substitution Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82
30
40
50
60
70
80
90
a0
b0
c0
d0	c1
e0	28	...
f0	16

Code 3.6: Byte Substitution

```

1 void SubBytes(u8* state) {
2     for (int i = 0; i < AES_BLOCK_SIZE; i++) {
3         state[i] = s_box[state[i]];
4     }
5 }
```

Code 3.7: Inverse Byte Substitution

```

1 void InvSubBytes(u8* state) {
2     for (int i = 0; i < AES_BLOCK_SIZE; i++) {
3         state[i] = inv_s_box[state[i]];
4     }
5 }
```

3.2.4 ShiftRows / InvShiftRows

- ShiftRows : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

X_0	X_4	X_8	X_{12}
X_1	X_5	X_9	X_{13}
X_2	X_6	X_{10}	X_{14}
X_3	X_7	X_{11}	X_{15}

 \Rightarrow

X_0	X_4	X_8	X_{12}
X_5	X_9	X_{13}	X_1
X_{10}	X_{14}	X_2	X_6
X_{15}	X_3	X_7	X_{11}

- InvShiftRows : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

X_0	X_4	X_8	X_{12}
X_1	X_5	X_9	X_{13}
X_2	X_6	X_{10}	X_{14}
X_3	X_7	X_{11}	X_{15}

 \Rightarrow

X_0	X_4	X_8	X_{12}
X_{13}	X_1	X_5	X_9
X_{10}	X_{14}	X_2	X_6
X_7	X_{11}	X_{15}	X_3

Code 3.8: ShiftRows

```

1 void ShiftRows(u8* state) {
2     u8 temp;
3
4     // Row 1: shift left by 1
5     temp = state[1];
6     state[1] = state[5];
7     state[5] = state[9];
8     state[9] = state[13];
9     state[13] = temp;
10
11    // Row 2: shift left by 2
12    temp = state[2];
13    state[2] = state[10];
14    state[10] = temp;
15    temp = state[6];
16    state[6] = state[14];
17    state[14] = temp;
18
19    // Row 3: shift left by 3 (or right by 1)
20    temp = state[15];
21    state[15] = state[11];
22    state[11] = state[7];
23    state[7] = state[3];
24    state[3] = temp;
25 }

```

Code 3.9: Inverse ShiftRows

```
1 void InvShiftRows(u8* state) {
2     u8 temp;
3
4     // Row 1: shift left by 3 (or right by 1)
5     temp = state[13];
6     state[13] = state[9];
7     state[9] = state[5];
8     state[5] = state[1];
9     state[1] = temp;
10
11    // Row 2: shift left by 2
12    temp = state[2];
13    state[2] = state[10];
14    state[10] = temp;
15    temp = state[6];
16    state[6] = state[14];
17    state[14] = temp;
18
19    // Row 3: shift left by 1
20    temp = state[3];
21    state[3] = state[7];
22    state[7] = state[11];
23    state[11] = state[15];
24    state[15] = temp;
25 }
```

3.2.5 MixColumns / InvMixColumns

- Multiplication in the finite field $GF(2^8)$.

$$\text{MUL}_{GF(2^8)} : \{\mathbf{0}, \mathbf{1}\}^8 \times \{\mathbf{0}, \mathbf{1}\}^8 \rightarrow \{\mathbf{0}, \mathbf{1}\}^8.$$

Here,

$$\{\mathbf{0}, \mathbf{1}\}^8 \simeq GF(2^8) = \mathbb{F}_{2^8} := \mathbb{F}_2[z]/(z^8 + z^4 + z^3 + z + 1) = \left\{ a_7 z^7 + \dots + a_1 z + a_0 : a_i \in \mathbb{F}_2 \right\}.$$

Note that

$$a(z) \times b(z) := a(z) \times b(z) \bmod (z^8 + z^4 + z^3 + z + 1)$$

Note. Given two polynomials $a(x)$ and $b(x)$ in $GF(2^8)$:

$$\begin{aligned} a(x) &= a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0, \\ b(x) &= b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0. \end{aligned}$$

The algorithm performs polynomial multiplication in the finite field $GF(2^8)$. It uses a shift-and-add method, with an additional reduction step modulo an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

1. Initialization: Set $p(x) = 0$ to initialize the product polynomial.
2. Iterate over each bit of $b(x)$, from LSB to MSB.
 - (i) If the current bit b_i of $b(x)$ is 1, update $p(x)$ as $p(x) \oplus a(x)$. In $GF(2^8)$, addition is equivalent to the XOR operation:

$$p(x) = p(x) \oplus a(x).$$

- (ii) Shift $a(x)$ left by 1 (multiply by x), increasing its degree by 1:

$$a(x) = a(x) \cdot x.$$

- (iii) If the coefficient of x^8 in $a(x)$ is 1, reduce $a(x)$ by $m(x)$ to keep the degree under 8:

$$a(x) = a(x) \oplus m(x).$$

- (iv) Shift $b(x)$ right by 1 (divide by x) for the next iteration:

$$b(x) = b(x) / x.$$

3. After all bits of $b(x)$ are processed, $p(x)$ be the product of $a(x)$ and $b(x)$ modulo $m(x)$.

Note (Modular Reduction in $GF(2^8)$ using XOR). In the context of multiplication in the binary finite field $GF(2^8)$, modular reduction ensures that results of operations remain within the field. The use of XOR for modular reduction is due to the properties of polynomial arithmetic over $GF(2)$ and the representation of elements in $GF(2^8)$.

– **Polynomial Representation in $GF(2^8)$:**

1. **Elements as Polynomials:** Each element in $GF(2^8)$ can be represented as a polynomial of degree less than 8, where each coefficient is either 0 or 1, i.e.,

$$GF(2^8) = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1) = \{a_7x^7 + \dots + a_1x + a_0 : a_i \in \mathbb{F}_2\}.$$

This corresponds to an 8-bit binary number, with each bit representing a coefficient of the polynomial, i.e.,

$$a_7x^7 + \dots + a_1x + a_0 \iff (a_7 \dots a_1a_0)_2.$$

2. **Binary Operations:** In $GF(2)$, addition and subtraction are equivalent to the XOR operation, since $1 + 1 = 0$ in this field, the same as $1 \oplus 1$.

– **Modular Reduction with an Irreducible Polynomial**

1. **Irreducible Polynomial:** In $GF(2^8)$, an irreducible polynomial of degree 8, typically $p(x) = x^8 + x^4 + x^3 + x + 1$ (represented as 0x11b in binary), is used for modular reduction.
 2. **Modular Reduction Process:** After multiplying two polynomials, if the resulting polynomial's degree is 8 or higher, it must be reduced modulo the irreducible polynomial to ensure the result remains a polynomial of degree less than 8, thus staying within $GF(2^8)$.
 3. **XOR for Reduction:** XOR is used for modular reduction in $GF(2^8)$ because polynomial subtraction in $GF(2)$ is performed by XORing coefficients.
- Given two elements in $GF(2^8)$, $a(x)$ and $b(x)$, their product is $c(x) = a(x) \cdot b(x)$. If $\deg(c(x)) \geq 8$, then $c(x)$ must be reduced modulo the irreducible polynomial $p(x)$. This is achieved by XORing the coefficients of $c(x)$ and $p(x)$:

$$c(x) = a(x) \cdot b(x) \mod p(x)$$

If $c(x)$ has a term x^8 or higher, we subtract $p(x)$ from $c(x)$ to reduce its degree. In $GF(2)$, subtraction is equivalent to addition, performed by XORing coefficients:

$$c'(x) = c(x) \oplus p(x)$$

This operation effectively eliminates the term x^8 (or higher) in $c(x)$, ensuring that the result remains within $GF(2^8)$. Consider the product of two polynomials $a(x)$ and $b(x)$ in $GF(2^8)$:

$$a(x) = x^6 + x^4 + x^2 + x + 1 \quad \text{and} \quad b(x) = x^7 + x + 1$$

The product $c(x) = a(x) \cdot b(x)$ might yield a polynomial of degree 8 or higher. To reduce $c(x)$ modulo $p(x) = x^8 + x^4 + x^3 + x + 1$, we perform XOR between the coefficients of $c(x)$ and $p(x)$, ensuring the result stays within $GF(2^8)$.

Code 3.10: Multiplication in $GF(2^8)$

```

1  u8 MUL_GF256(u8 a, u8 b) {
2      u8 res = 0;
3      // Mask for detecting the MSB (0x80 = 0b10000000)
4      u8 MSB_mask = 0x80;
5      u8 MSB;
6      /*
7       * The reduction polynomial
8       * (x^8 + x^4 + x^3 + x + 1) = 0b100011011
9       * for AES, represented in hexadecimal
10     */
11     u8 modulo = 0x1B;
12
13     for (int i = 0; i < 8; i++) {
14         // Add a to result if LSB(b)=1
15         if (b & 1)
16             res ^= a;
17
18         MSB = a & MSB_mask; // Store the MSB of a
19         a <<= 1; // Multiplying it by x effectively
20
21         // Reduce the result modulo the reduction polynomial
22         if (MSB)
23             a ^= modulo;
24
25         b >>= 1; // Moving to the next bit
26     }
27
28     return res;
29 }
30
31 #define MUL_GF256(a, b) ({ \
32     u8 res = 0; \
33     u8 MSB_mask = 0x80; \
34     u8 MSB; \
35     u8 modulo = 0x1B; \
36     u8 temp_a = (a); \
37     u8 temp_b = (b); \
38     for (int i = 0; i < 8; i++) { \
39         if (temp_b & 1) \
40             res ^= temp_a; \
41         MSB = temp_a & MSB_mask; \
42         temp_a <<= 1; \
43         if (MSB) \
44             temp_a ^= modulo; \
45         temp_b >>= 1; \
46     } \
47     res; \
48 })

```

- MixColumns : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

$$\text{MixColumns} \left(\begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix} \right) := \begin{pmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{pmatrix} \begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix}.$$

- InvMixColumns : $\{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ is defined by

$$\text{MixColumns} \left(\begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix} \right) := \begin{pmatrix} 0x0e & 0x0b & 0x0d & 0x09 \\ 0x09 & 0x0e & 0x0b & 0x0d \\ 0x0d & 0x09 & 0x0e & 0x0b \\ 0x0b & 0x0d & 0x09 & 0x0e \end{pmatrix} \begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix}.$$

Code 3.11: MixColumns

```

1 void MixColumns(u8* state) {
2     u8 temp[4];
3     // Multiply and add the elements in the column
4     // by the fixed polynomial
5     for (int i = 0; i < 4; i++) {
6         temp[0] =
7             MUL_GF256(0x02, state[i * 4]) ^
8             MUL_GF256(0x03, state[i * 4 + 1]) ^
9             state[i * 4 + 2] ^
10            state[i * 4 + 3];
11
12        temp[1] =
13            state[i * 4] ^
14            MUL_GF256(0x02, state[i * 4 + 1]) ^
15            MUL_GF256(0x03, state[i * 4 + 2]) ^
16            state[i * 4 + 3];
17
18        temp[2] =
19            state[i * 4] ^
20            state[i * 4 + 1] ^
21            MUL_GF256(0x02, state[i * 4 + 2]) ^
22            MUL_GF256(0x03, state[i * 4 + 3]);
23
24        temp[3] =
25            MUL_GF256(0x03, state[i * 4]) ^
26            state[i * 4 + 1] ^
27            state[i * 4 + 2] ^
28            MUL_GF256(0x02, state[i * 4 + 3]);
29
30        // Copy the mixed column back to the state
31        for (int j = 0; j < 4; j++)
32            state[i * 4 + j] = temp[j];
33    }
34 }

```

Code 3.12: Inverse MixColumns

```

1 void InvMixColumns(u8* state) {
2     u8 temp[4];
3
4     for (int i = 0; i < 4; i++) {
5         temp[0] =
6             MUL_GF256(0x0e, state[i * 4]) ^
7             MUL_GF256(0x0b, state[i * 4 + 1]) ^
8             MUL_GF256(0x0d, state[i * 4 + 2]) ^
9             MUL_GF256(0x09, state[i * 4 + 3]);
10
11         temp[1] =
12             MUL_GF256(0x09, state[i * 4]) ^
13             MUL_GF256(0x0e, state[i * 4 + 1]) ^
14             MUL_GF256(0x0b, state[i * 4 + 2]) ^
15             MUL_GF256(0x0d, state[i * 4 + 3]);
16
17         temp[2] =
18             MUL_GF256(0x0d, state[i * 4]) ^
19             MUL_GF256(0x09, state[i * 4 + 1]) ^
20             MUL_GF256(0x0e, state[i * 4 + 2]) ^
21             MUL_GF256(0x0b, state[i * 4 + 3]);
22
23         temp[3] =
24             MUL_GF256(0x0b, state[i * 4]) ^
25             MUL_GF256(0x0d, state[i * 4 + 1]) ^
26             MUL_GF256(0x09, state[i * 4 + 2]) ^
27             MUL_GF256(0x0e, state[i * 4 + 3]);
28
29         for (int j = 0; j < 4; j++)
30             state[i * 4 + j] = temp[j];
31     }
32 }

```

Chapter 4

AES - 128 / 192 / 256 (Byte Version)

4.1 Specification

Table 4.1: Parameters of the Block Cipher AES (1-word = 32-bit)

Algorithms	Block Size (N_b -word)	Key Length (N_k -word)	Number of Rounds (N_r)	Round-Key Length (word)	Number of Round-Keys ($N_r + 1$)	Total Size of Round-Keys ($N_b(N_r + 1)$)
AES-128	4	4 (4·32-bit)	10	4	11	44 (176-byte)
AES-192	4	6 (6·32-bit)	12	4	13	52 (208-byte)
AES-256	4	8 (8·32-bit)	14	4	15	60 (240-byte)

Code 4.1: Configuration in C

```
1 // Define macros for AES key length
2 #define AES_VERSION 128 // Can be 128, 192, or 256
3 // Define macro for AES block size
4 #define AES_BLOCK_SIZE 16
5
6 // Define Nk and Nr based on AES key length
7 #if AES_VERSION == 128
8     #define Nk 4
9 #elif AES_VERSION == 192
10    #define Nk 6
11 #elif AES_VERSION == 256
12    #define Nk 8
13 #else
14    #error "Invalid AES ky length"
15 #endif
16
17 #define Nr (Nk + 6) // 10 / 12 / 14
18 #define ROUND_KEYS_SIZE (16 * (Nr + 1)) // 176 / 208 / 240
```

Code 4.2: Configuration in Rust

```
1 // Define a constant for the AES key length.
2 pub const AES_VERSION: u32 = 128; // Can be 128, 192, or 256
3
4 // Define constant for AES block size
5 pub const AES_BLOCK_SIZE: usize = 16;
6
7 // Define constants Nk and Nr based on AES key length
8 pub const NK: usize = match AES_VERSION {
9     128 => 4,
10    192 => 6,
11    256 => 8,
12    _ => panic!("Invalid AES key length"),
13 };
14
15 pub const NR: usize = NK + 6;
16 pub const ROUND_KEYS_SIZE: usize = 16 * (NR + 1);
```

4.2 Key Expansion (General Version)

Algorithm 6: Key Schedule (General Version)

Input: User-key $uk = (uk_0, \dots, uk_{N_k-1})$ ($uk_i \in \{0, 1\}^8$); // uk is 16/24/32-byte

Output: Round-key $\{rk_i\}_{i=0}^{4(N_r+1)-1}$ ($rk_i \in \{0, 1\}^{32}$)

/* $\{rk_i\}_{i=0}^{4(N_r+1)-1}$ is 176/208/240-byte */

```

1  $l \leftarrow N_k/4;$  //  $l = 4, 6, 8$ 
2 for  $i = 0$  to  $l - 1$  do
3    $rk_i \leftarrow uk_{4i} \parallel uk_{4i+1} \parallel uk_{4i+2} \parallel uk_{4i+3};$ 
4 end
5 for  $i = l$  to  $4(N_r + 1) - 1$  do
6    $t \leftarrow rk_{i-1};$ 
7   if  $i \bmod l = 0$  then
8      $t \leftarrow (\text{SubWord} \circ \text{RotWord})(t);$ 
9      $t \leftarrow t \oplus_{32} (\text{rCon}_{i/l} \parallel 0x00 \parallel 0x00 \parallel 0x00);$ 
10  else if  $l > 6 \ \&\& \ i \bmod l = 4$  then
11     $t \leftarrow \text{SubWord}(t);$ 
12  end
13   $rk_i \leftarrow rk_{i-l} \oplus_{32} t;$ 
14 end

```

Code 4.3: Key Expansion in C (General ver.)

```

1 void KeyExpansion(const u8* uKey, u32* rKey) {
2     u32 temp;
3
4     for (int i = 0; i < Nk; i++) {
5         rKey[i] = (u32)uKey[4*i] << 0x18 |
6                 (u32)uKey[4*i+1] << 0x10 |
7                 (u32)uKey[4*i+2] << 0x08 |
8                 (u32)uKey[4*i+3];
9     }
10
11    for (int i = Nk; i < (Nr + 1) * 4; i++) {
12        temp = rKey[i - 1];
13        if (i % Nk == 0) {
14            temp = SubWord(RotWord(temp)) ^ rCon[i / Nk - 1];
15        } else if (Nk > 6 && i % Nk == 4) {
16            // Additional S-box transformation for AES-256
17            temp = SubWord(temp);
18        }
19        rKey[i] = rKey[i - Nk] ^ temp;
20    }
21 }

```

Code 4.4: Key Expansion Test

```

1 void RANDOM_KEY_GENERATION(u8* key) {
2     srand((u32)time(NULL));
3
4     // Initialize pointer to the start of the key array
5     u8* p = key;
6
7     // Set the counter to 16 bytes
8     int cnt = 0;
9
10    // Loop until all 16 bytes are filled
11    while (cnt < AES_BLOCK_SIZE) {
12        *p = rand() & 0xff; // Assign a random byte (0 to 255)
13        p++;                // Move to the next byte
14        cnt++;              // Decrement the byte count
15    }
16 }
17
18 void KeyExpansionTest() {
19     u8 uKey[AES_BLOCK_SIZE] = { 0x00, };
20     RANDOM_KEY_GENERATION(uKey);
21     // u8 uKey[AES_BLOCK_SIZE] = {
22     //     0x2b, 0x7e, 0x15, 0x16, 0x28, 0xae, 0xd2, 0xa6,
23     //     0xab, 0xf7, 0x15, 0x88, 0x09, 0xcf, 0x4f, 0x3c
24     // };
25     for (int i = 0; i < AES_BLOCK_SIZE; i++) {
26         printf("%02x", uKey[i]);
27     } printf("\n");
28
29     u32 rKeys[ROUND_KEYS_SIZE / sizeof(u32)];
30     KeyExpansion(uKey, rKeys);
31     for (int i = 0; i < ROUND_KEYS_SIZE / sizeof(u32); i++) {
32         printf("%08x\n", rKeys[i]);
33     }
34 }
35
36 int main() {
37     KeyExpansionTest();
38     return 0;
39 }

```

4.3 8-bit AES - 128 / 192 / 256

Algorithm 7: Encryption of 8-bit AES

Input: block $\text{src} \in \{0, 1\}^{128}$, round-keys $\{rk_i\}_{i=0}^{N_r+1}$ ($rk_i \in \{0, 1\}^{32 \times 4}$)

Output: block $\text{dst} \in \{0, 1\}^{128}$

```

1  $t \leftarrow \text{AddRoundKey}(\text{src}, rk_0);$            //  $\text{AddRoundKey}: \{0, 1\}^{8 \times 16} \times \{0, 1\}^{32 \times 4} \rightarrow \{0, 1\}^{8 \times 16}$ 
2 for  $i \leftarrow 1$  to  $N_r - 1$  do
3    $t \leftarrow \text{SubBytes}(t);$                      //  $\text{SubBytes}: \{0, 1\}^{8 \times 16} \rightarrow \{0, 1\}^{8 \times 16}$ 
4    $t \leftarrow \text{ShiftRows}(t);$                    //  $\text{ShiftRows}: \{0, 1\}^{8 \times 16} \rightarrow \{0, 1\}^{8 \times 16}$ 
5    $t \leftarrow \text{MixColumns}(t);$                  //  $\text{MixColumns}: \{0, 1\}^{8 \times 16} \rightarrow \{0, 1\}^{8 \times 16}$ 
6    $t \leftarrow \text{AddRoundKey}(t, rk_i);$ 
7 end
8  $t \leftarrow \text{SubBytes}(t);$ 
9  $t \leftarrow \text{ShiftRows}(t);$ 
10  $t \leftarrow \text{AddRoundKey}(t, rk_{N_r});$ 
11  $\text{dst} \leftarrow t;$ 
12 return  $\text{dst};$ 

```

Code 4.5: 8-bit AES Encryption

```

1 void AES_Encrypt(const u8* plaintext, const u8* key,
2   u8* ciphertext) {
3   // AES-128/192/256: roundKey[44]/roundKey[52]/roundKey[60]
4   u32 roundKey[ROUND_KEYS_SIZE / sizeof(u32)];
5   u8 state[AES_BLOCK_SIZE]; // state[16]
6
7   // Copy plaintext to state
8   for (int i = 0; i < AES_BLOCK_SIZE; i++)
9     state[i] = plaintext[i];
10
11   KeyExpansion(key, roundKey);
12
13   // 0: roundKey[ 0] | roundKey[1] | roundKey[ 2] | roundKey[ 3]
14   AddRoundKey(state, roundKey); // Initial round
15
16   for (int round = 1; round <= Nr; round++) { // Main rounds
17     SubBytes(state); ShiftRows(state);
18     if (round != Nr) MixColumns(state);
19     // 1: roundKey[ 4] | roundKey[5] | roundKey[ 6] | roundKey[ 7]
20     // 2: roundKey[ 8] | roundKey[9] | roundKey[10] | roundKey[ 11]
21     // i: roundKey[4*i] | ... | ... | roundKey[4*i+3]
22     AddRoundKey(state, roundKey + 4 * round);
23   }
24
25   // Copy state to ciphertext
26   for (int i = 0; i < AES_BLOCK_SIZE; i++)
27     ciphertext[i] = state[i];
28 }

```


Algorithm 8: Decryption of 8-bit AES**Input:** block $\text{src} \in \{0, 1\}^{128}$, round-keys $\{rk_i\}_{i=0}^{N_r+1}$ ($rk_i \in \{0, 1\}^{32 \times 4}$)**Output:** block $\text{dst} \in \{0, 1\}^{128}$

```

1  $t \leftarrow \text{AddRoundKey}(\text{src}, rk_{N_r});$ 
2 for  $i \leftarrow N_r - 1$  to 1 do
3    $t \leftarrow \text{InvShiftRows}(t);$ 
4    $t \leftarrow \text{InvSubBytes}(t);$ 
5    $t \leftarrow \text{AddRoundKey}(t, rk_i);$ 
6    $t \leftarrow \text{InvMixColumns}(t);$ 
7 end
8  $t \leftarrow \text{InvShiftRows}(t);$ 
9  $t \leftarrow \text{InvSubBytes}(t);$ 
10  $t \leftarrow \text{AddRoundKey}(t, rk_0);$ 
11  $\text{dst} \leftarrow t;$ 
12 return  $\text{dst};$ 

```

Code 4.6: 8-bit AES Decryption

```

1 void AES_Decrypt(const u8* ciphertext, const u8* key,
2   u8* plaintext) {
3   u32 roundKey[ROUND_KEYS_SIZE / sizeof(u32)];
4   u8 state[AES_BLOCK_SIZE];
5
6   KeyExpansion(key, roundKey);
7
8   for (int i = 0; i < AES_BLOCK_SIZE; i++)
9     state[i] = ciphertext[i];
10
11   // Initial round with the last round key
12   AddRoundKey(state, roundKey + 4 * Nr);
13
14   // Main rounds in reverse order
15   for (int round = Nr - 1; round >= 0; round--) {
16     InvShiftRows(state);
17     InvSubBytes(state);
18     // i: roundKey[4*i] | ... | roundKey[4*i+3]
19     // 1: roundKey[ 4] | roundKey[5] | roundKey[ 6] | roundKey[ 7]
20     // 0: roundKey[ 0] | roundKey[1] | roundKey[ 2] | roundKey[ 3]
21     AddRoundKey(state, roundKey + 4 * round);
22     if (round != 0)
23       InvMixColumns(state);
24   }
25
26   for (int i = 0; i < AES_BLOCK_SIZE; i++)
27     plaintext[i] = state[i];
28 }

```

Chapter 5

Pre-Computation using SubMix

5.1 SubMix and InvSubInvMix

- $\text{SubMix} : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ and $\text{InvSubInvMix} : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ are defined by

$$\text{SubMix} := \text{MixColumns} \circ \text{SubBytes}$$

$$\text{InvSubInvMix} := \text{InvMixColumns} \circ \text{InvSubBytes}.$$

Algorithm 9: Encryption and Decryption of AES using SubMix and InvSubInvMix

Input: block $\text{src} \in \{0, 1\}^{128}$, round-keys $\{rk_i\}_{i=0}^{N_r+1}$ ($rk_i \in \{0, 1\}^{128}$)

Output: block $\text{dst} \in \{0, 1\}^{128}$

1 **Function** AES_ENC:

```
2    $t \leftarrow \text{src};$ 
3    $t \leftarrow \text{AddRoundKey}(t, rk_0);$ 
4   for  $i \leftarrow 1$  to  $N_r - 1$  do
5        $t \leftarrow \text{ShiftRows}(t);$ 
6        $t \leftarrow \text{SubMix}(t);$ 
7        $t \leftarrow \text{AddRoundKey}(t, rk_i);$ 
8   end
9    $t \leftarrow \text{SubBytes}(t);$ 
10   $t \leftarrow \text{ShiftRows}(t);$ 
11   $t \leftarrow \text{AddRoundKey}(t, rk_{N_r});$ 
12   $\text{dst} \leftarrow t;$ 
13  return  $\text{dst};$ 
14 end
```

1 **Function** AES_DEC:

```
2    $t \leftarrow \text{src};$ 
3    $t \leftarrow \text{AddRoundKey}(t, rk_{N_r});$ 
4   for  $i \leftarrow N_r - 1$  downto 1 do
5        $t \leftarrow \text{InvShiftRows}(t);$ 
6        $t \leftarrow \text{InvSubInvMix}(t);$ 
7        $t' \leftarrow \text{InvMixColumns}(rk_i);$ 
8        $t \leftarrow \text{AddRoundKey}(t, t');$ 
9   end
10   $t \leftarrow \text{InvShiftRows}(t);$ 
11   $t \leftarrow \text{InvSubBytes}(t);$ 
12   $t \leftarrow \text{AddRoundKey}(t, rk_0);$ 
13   $\text{dst} \leftarrow t;$ 
14  return  $\text{dst};$ 
15 end
```

5.2 8×32 Table Look Up

Convert the 8-bit string $\{X_i\}_{i=0}^{15}$ ($X_i \in \{0, 1\}^8$) into a 32-bit string $\{W_i\}_{i=0}^3$ ($W_i \in \{0, 1\}^{32}$) as follows:

$$W_i := (X_{4i} \ll 24) \parallel (X_{4i+1} \ll 16) \parallel (X_{4i+2} \ll 8) \parallel (X_{4i+3}) \in \{0, 1\}^{32}$$

for $i = 0, 1, 2, 3$. In other words,

X_0	$(W_0 \gg 0x18) \& 0xff$	X_4	$(W_1 \gg 0x18) \& 0xff$
X_1	$(W_0 \gg 0x10) \& 0xff$	X_5	$(W_1 \gg 0x10) \& 0xff$
X_2	$(W_0 \gg 0x08) \& 0xff$	X_6	$(W_1 \gg 0x08) \& 0xff$
X_3	$(W_0) \& 0xff$	X_7	$(W_1) \& 0xff$
X_8	$(W_2 \gg 0x18) \& 0xff$	X_{12}	$(W_3 \gg 0x18) \& 0xff$
X_9	$(W_2 \gg 0x10) \& 0xff$	X_{13}	$(W_3 \gg 0x10) \& 0xff$
X_{10}	$(W_2 \gg 0x08) \& 0xff$	X_{14}	$(W_3 \gg 0x08) \& 0xff$
X_{11}	$(W_2) \& 0xff$	X_{15}	$(W_3) \& 0xff$

Note that

X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}
W_0				W_1				W_2				W_3			

Algorithm 10: SubMix and InvSubInvMix

Input: $(W_0, W_1, W_2, W_3) \in \{0, 1\}^{128=32 \times 4}$

Output: $(V_0, V_1, V_2, V_3) \in \{0, 1\}^{128=32 \times 4}$

1 **Function** SubMix:

2 **for** $i \leftarrow 0$ **to** 3 **do**

3 $V_i \leftarrow Te_0((W_i \gg 0x18) \& 0xff)$
4 $\oplus_{32} Te_1((W_i \gg 0x10) \& 0xff)$
5 $\oplus_{32} Te_2((W_i \gg 0x08) \& 0xff)$
6 $\oplus_{32} Te_3(W_i \& 0xff);$

7 **end**

8 **return** $(V_0, V_1, V_2, V_3);$

9 **end**

Input: $(W_0, W_1, W_2, W_3) \in \{0, 1\}^{128=32 \times 4}$

Output: $(U_0, U_1, U_2, U_3) \in \{0, 1\}^{128=32 \times 4}$

1 **Function** InvSubInvMix:

2 **for** $i \leftarrow 0$ **to** 3 **do**

3 $U_i \leftarrow Td_0((W_i \gg 0x18) \& 0xff)$
4 $\oplus_{32} Td_1((W_i \gg 0x10) \& 0xff)$
5 $\oplus_{32} Td_2((W_i \gg 0x08) \& 0xff)$
6 $\oplus_{32} Td_3(W_i \& 0xff);$

7 **end**

8 **return** $(U_0, U_1, U_2, U_3);$

9 **end**

5.3 Generation of 8×32 Tables

Note that

$$\begin{aligned}
 \begin{pmatrix} V_0 & V_4 & V_8 & V_{12} \\ V_1 & V_5 & V_9 & V_{13} \\ V_2 & V_6 & V_{10} & V_{14} \\ V_3 & V_7 & V_{11} & V_{15} \end{pmatrix} &= \text{SubMix} \left(\begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix} \right) := \\
 &\begin{pmatrix} \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} \\ \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} \end{pmatrix} \begin{pmatrix} s(X_0) & s(X_4) & s(X_8) & s(X_{12}) \\ s(X_1) & s(X_5) & s(X_9) & s(X_{13}) \\ s(X_2) & s(X_6) & s(X_{10}) & s(X_{14}) \\ s(X_3) & s(X_7) & s(X_{11}) & s(X_{15}) \end{pmatrix}, \\
 \begin{pmatrix} U_0 & V_4 & U_8 & U_{12} \\ U_1 & V_5 & U_9 & U_{13} \\ U_2 & V_6 & U_{10} & U_{14} \\ U_3 & V_7 & U_{11} & U_{15} \end{pmatrix} &= \text{InvSubInvMix} \left(\begin{pmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{pmatrix} \right) := \\
 &\begin{pmatrix} \mathbf{0x0e} & \mathbf{0x0b} & \mathbf{0x0d} & \mathbf{0x09} \\ \mathbf{0x09} & \mathbf{0x0e} & \mathbf{0x0b} & \mathbf{0x0d} \\ \mathbf{0x0d} & \mathbf{0x09} & \mathbf{0x0e} & \mathbf{0x0b} \\ \mathbf{0x0b} & \mathbf{0x0d} & \mathbf{0x09} & \mathbf{0x0e} \end{pmatrix} \begin{pmatrix} s^{-1}(X_0) & s^{-1}(X_4) & s^{-1}(X_8) & s^{-1}(X_{12}) \\ s^{-1}(X_1) & s^{-1}(X_5) & s^{-1}(X_9) & s^{-1}(X_{13}) \\ s^{-1}(X_2) & s^{-1}(X_6) & s^{-1}(X_{10}) & s^{-1}(X_{14}) \\ s^{-1}(X_3) & s^{-1}(X_7) & s^{-1}(X_{11}) & s^{-1}(X_{15}) \end{pmatrix}.
 \end{aligned}$$

Then

$$\begin{aligned}
 \begin{pmatrix} V_{4i} \\ V_{4i+1} \\ V_{4i+2} \\ V_{4i+3} \end{pmatrix} &= \begin{pmatrix} \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} & \mathbf{0x01} \\ \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} & \mathbf{0x03} \\ \mathbf{0x03} & \mathbf{0x01} & \mathbf{0x01} & \mathbf{0x02} \end{pmatrix} \begin{pmatrix} s(X_{4i}) \\ s(X_{4i+1}) \\ s(X_{4i+2}) \\ s(X_{4i+3}) \end{pmatrix} \\
 &= s(X_{4i}) \begin{pmatrix} \mathbf{0x02} \\ \mathbf{0x01} \\ \mathbf{0x01} \\ \mathbf{0x03} \end{pmatrix} \oplus_{32} s(X_{4i+1}) \begin{pmatrix} \mathbf{0x03} \\ \mathbf{0x02} \\ \mathbf{0x01} \\ \mathbf{0x01} \end{pmatrix} \oplus_{32} s(X_{4i+2}) \begin{pmatrix} \mathbf{0x01} \\ \mathbf{0x03} \\ \mathbf{0x02} \\ \mathbf{0x01} \end{pmatrix} \oplus_{32} s(X_{4i+3}) \begin{pmatrix} \mathbf{0x01} \\ \mathbf{0x01} \\ \mathbf{0x03} \\ \mathbf{0x02} \end{pmatrix}, \\
 \begin{pmatrix} U_{4i} \\ U_{4i+1} \\ U_{4i+2} \\ U_{4i+3} \end{pmatrix} &= \begin{pmatrix} \mathbf{0x0e} & \mathbf{0x0b} & \mathbf{0x0d} & \mathbf{0x09} \\ \mathbf{0x09} & \mathbf{0x0e} & \mathbf{0x0b} & \mathbf{0x0d} \\ \mathbf{0x0d} & \mathbf{0x09} & \mathbf{0x0e} & \mathbf{0x0b} \\ \mathbf{0x0b} & \mathbf{0x0d} & \mathbf{0x09} & \mathbf{0x0e} \end{pmatrix} \begin{pmatrix} s^{-1}(X_{4i}) \\ s^{-1}(X_{4i+1}) \\ s^{-1}(X_{4i+2}) \\ s^{-1}(X_{4i+3}) \end{pmatrix} \\
 &= s^{-1}(X_{4i}) \begin{pmatrix} \mathbf{0x0e} \\ \mathbf{0x09} \\ \mathbf{0x0d} \\ \mathbf{0x0b} \end{pmatrix} \oplus s^{-1}(X_{4i+1}) \begin{pmatrix} \mathbf{0x0b} \\ \mathbf{0x0e} \\ \mathbf{0x09} \\ \mathbf{0x0d} \end{pmatrix} \oplus s^{-1}(X_{4i+2}) \begin{pmatrix} \mathbf{0x0d} \\ \mathbf{0x0b} \\ \mathbf{0x0e} \\ \mathbf{0x09} \end{pmatrix} \oplus s^{-1}(X_{4i+3}) \begin{pmatrix} \mathbf{0x09} \\ \mathbf{0x0d} \\ \mathbf{0x0b} \\ \mathbf{0x0e} \end{pmatrix}.
 \end{aligned}$$

We define $Te_i/Td_i : \{\mathbf{0}, \mathbf{1}\}^8 \rightarrow \{\mathbf{0}, \mathbf{1}\}^{32}$ ($i \in \{0, 1, 2, 3\}$) as follows:

$$\begin{aligned} Te_0(X) &:= \left(\mathbf{0x02} \otimes_8 s(X), s(X), s(X), \mathbf{0x03} \otimes_8 s(X) \right), \\ Te_1(X) &:= \left(\mathbf{0x03} \otimes_8 s(X), \mathbf{0x02} \otimes_8 s(X), s(X), s(X) \right), \\ Te_2(X) &:= \left(s(X), \mathbf{0x03} \otimes_8 s(X), \mathbf{0x02} \otimes_8 s(X), s(X) \right), \\ Te_3(X) &:= \left(s(X), s(X), \mathbf{0x03} \otimes_8 s(X), \mathbf{0x02} \otimes_8 s(X) \right), \end{aligned}$$

and

$$\begin{aligned} Td_0(X) &:= \left(\mathbf{0x0e} \otimes_8 s^{-1}(X), \mathbf{0x09} \otimes_8 s^{-1}(X), \mathbf{0x0d} \otimes_8 s^{-1}(X), \mathbf{0x0b} \otimes_8 s^{-1}(X) \right), \\ Td_1(X) &:= \left(\mathbf{0x0b} \otimes_8 s^{-1}(X), \mathbf{0x0e} \otimes_8 s^{-1}(X), \mathbf{0x09} \otimes_8 s^{-1}(X), \mathbf{0x0d} \otimes_8 s^{-1}(X) \right), \\ Td_2(X) &:= \left(\mathbf{0x0d} \otimes_8 s^{-1}(X), \mathbf{0x0b} \otimes_8 s^{-1}(X), \mathbf{0x0e} \otimes_8 s^{-1}(X), \mathbf{0x09} \otimes_8 s^{-1}(X) \right), \\ Td_3(X) &:= \left(\mathbf{0x09} \otimes_8 s^{-1}(X), \mathbf{0x0d} \otimes_8 s^{-1}(X), \mathbf{0x0b} \otimes_8 s^{-1}(X), \mathbf{0x0e} \otimes_8 s^{-1}(X) \right). \end{aligned}$$

SubMix/InvSubInvMix : $\{\mathbf{0}, \mathbf{1}\}^{128} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{128}$ are computed as follows:

$$\begin{aligned} \text{SubMix}(W_0, W_1, W_2, W_3) &:= (V_0, V_1, V_2, V_3), \\ \text{InvSubInvMix}(W_0, W_1, W_2, W_3) &:= (U_0, U_1, U_2, U_3) \end{aligned}$$

$$\text{where } \begin{cases} W_0 := X_0 \parallel X_1 \parallel X_2 \parallel X_3 \\ W_1 := X_4 \parallel X_5 \parallel X_6 \parallel X_7 \\ W_2 := X_8 \parallel X_9 \parallel X_{10} \parallel X_{11} \\ W_3 := X_{12} \parallel X_{13} \parallel X_{14} \parallel X_{15} \end{cases} \quad (W_i \in \{\mathbf{0}, \mathbf{1}\}^{32}) \text{ and}$$

$$\begin{aligned} V_0 &:= Te_0(X_0) \oplus_{32} Te_1(X_1) \oplus_{32} Te_2(X_2) \oplus_{32} Te_3(X_3), \\ V_1 &:= Te_0(X_4) \oplus_{32} Te_1(X_5) \oplus_{32} Te_2(X_6) \oplus_{32} Te_3(X_7), \\ V_2 &:= Te_0(X_8) \oplus_{32} Te_1(X_9) \oplus_{32} Te_2(X_{10}) \oplus_{32} Te_3(X_{11}), \\ V_3 &:= Te_0(X_{12}) \oplus_{32} Te_1(X_{13}) \oplus_{32} Te_2(X_{14}) \oplus_{32} Te_3(X_{15}), \end{aligned}$$

$$\begin{aligned} U_0 &:= Td_0(X_0) \oplus_{32} Td_1(X_1) \oplus_{32} Td_2(X_2) \oplus_{32} Td_3(X_3), \\ U_1 &:= Td_0(X_4) \oplus_{32} Td_1(X_5) \oplus_{32} Td_2(X_6) \oplus_{32} Td_3(X_7), \\ U_2 &:= Td_0(X_8) \oplus_{32} Td_1(X_9) \oplus_{32} Td_2(X_{10}) \oplus_{32} Td_3(X_{11}), \\ U_3 &:= Td_0(X_{12}) \oplus_{32} Td_1(X_{13}) \oplus_{32} Td_2(X_{14}) \oplus_{32} Td_3(X_{15}). \end{aligned}$$

5.4 Implementation of SubMix and InvSubInvMix

Code 5.1: SubMix

```

1 void SubMix(u8* state) {
2     u32 temp[4];
3
4     // temp[0] = Te0[state[ 0]] ^ Te1[state[ 1]] ^
5     //           Te2[state[ 2]] ^ Te3[state[ 3]];
6     // temp[1] = Te0[state[ 4]] ^ Te1[state[ 5]] ^
7     //           Te2[state[ 6]] ^ Te3[state[ 7]];
8     // temp[2] = Te0[state[ 8]] ^ Te1[state[ 9]] ^
9     //           Te2[state[10]] ^ Te3[state[11]];
10    // temp[3] = Te0[state[11]] ^ Te1[state[12]] ^
11    //           Te2[state[13]] ^ Te3[state[14]];
12
13    for (int i = 0; i < 4; i++) {
14        temp[i] = Te0[state[4*i + 0]] ^
15                Te1[state[4*i + 1]] ^
16                Te2[state[4*i + 2]] ^
17                Te3[state[4*i + 3]];
18    }
19
20    for (int i = 0; i < 4; i++) {
21        state[4*i + 0] = (temp[i] >> 0x18) & 0xff;
22        state[4*i + 1] = (temp[i] >> 0x10) & 0xff;
23        state[4*i + 2] = (temp[i] >> 0x08) & 0xff;
24        state[4*i + 3] = temp[i] & 0xff;
25    }
26 }

```

Code 5.2: InvSubInvMix

```

1 void InvSubInvMix(u8* state) {
2     u32 temp[4];
3
4     for (int i = 0; i < 4; i++) {
5         temp[i] = Td0[state[4*i + 0]] ^
6                 Td1[state[4*i + 1]] ^
7                 Td2[state[4*i + 2]] ^
8                 Td3[state[4*i + 3]];
9     }
10
11    for (int i = 0; i < 4; i++) {
12        state[4*i + 0] = (temp[i] >> 0x18) & 0xff;
13        state[4*i + 1] = (temp[i] >> 0x10) & 0xff;
14        state[4*i + 2] = (temp[i] >> 0x08) & 0xff;
15        state[4*i + 3] = temp[i] & 0xff;
16    }
17 }

```

Chapter 6

32-bit AES

Code 6.1: SubWord applies the S-box to each byte of the input word

```
1  /* Table Annotation:
2  | i | Shift | Mask | Description |
3  |---|-----|-----|-----|
4  | 0 | 0x18 | 0xFF << 0x18 | Process most significant byte (1st)|
5  | 1 | 0x10 | 0xFF << 0x10 | Process 2nd byte |
6  | 2 | 0x08 | 0xFF << 0x08 | Process 3rd byte |
7  | 3 | 0x00 | 0xFF << 0x00 | Process least significant byte (4th)|
8  */
9
10 u32 SubWord(u32* word) {
11     u8 temp;
12     for (int i = 0; i < 4; i++) {
13         temp = Te3[(*word >> (0x18 - 0x08 * i)) & 0x000000ff];
14         *word &= ~(0xFF << (0x18 - 0x08 * i)); // Clear the byte
15         *word |= (temp & 0x000000ff) << (0x18 - 0x08 * i); // Set
16                                     the new value
17     }
18 }
```

Code 6.2: SubWord applies the S-box to each byte of the input word

```

1  u32 SubWord(u32 word) {
2      u8 temp0, temp1, temp2, temp3;
3
4      // Process the most significant byte (1st byte)
5      temp0 = Te3[(word >> 24) & 0x000000ff];
6      word &= 0x00ffffff; // Clear the most significant byte
7      word |= (temp0 & 0x000000ff) << 24; // Set the new value
8
9      // Process the 2nd byte
10     temp1 = Te3[(word >> 16) & 0x000000ff];
11     word &= 0xff00ffff; // Clear the 2nd byte
12     word |= (temp1 & 0x000000ff) << 16; // Set the new value
13
14     // Process the 3rd byte
15     temp2 = Te3[(word >> 8) & 0x000000ff];
16     word &= 0xffff00ff; // Clear the 3rd byte
17     word |= (temp2 & 0x000000ff) << 8; // Set the new value
18
19     // Process the least significant byte (4th byte)
20     temp3 = Te3[word & 0x000000ff];
21     word &= 0xffffffff00; // Clear the least significant byte
22     word |= (temp3 & 0x000000ff); // Set the new value
23
24     return word;
25 }

```

Code 6.3: SubWord applies the S-box to each byte of the input word

```

1  u32 SubWord(u32 word) {
2      // Apply the transformation to each byte and combine them
3      return (Te3[(word >> 0x18) & 0xff] & 0xff000000) |
4      (Te3[(word >> 0x10) & 0xff] & 0x00ff0000) |
5      (Te1[(word >> 0x08) & 0xff] & 0x0000ff00) |
6      (Te1[word & 0xff] & 0x000000ff );
7  }

```


Appendix A

Additional Data A

A.1 Substitution-BOX

```
1 static const u8 s_box[256] = {
2     0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5,
3     0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76,
4     0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0,
5     0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0,
6     0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc,
7     0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15,
8     0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a,
9     0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75,
10    0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0,
11    0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,
12    0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b,
13    0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf,
14    0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85,
15    0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8,
16    0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5,
17    0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2,
18    0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17,
19    0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73,
20    0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88,
21    0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,
22    0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c,
23    0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79,
24    0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9,
25    0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08,
26    0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6,
27    0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a,
28    0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e,
29    0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e,
30    0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94,
31    0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,
32    0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68,
33    0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16
34 };
```

```

1  static const u8 inv_s_box[256] = {
2      0x52, 0x09, 0x6a, 0xd5, 0x30, 0x36, 0xa5, 0x38,
3      0xbf, 0x40, 0xa3, 0x9e, 0x81, 0xf3, 0xd7, 0xfb,
4      0x7c, 0xe3, 0x39, 0x82, 0x9b, 0x2f, 0xff, 0x87,
5      0x34, 0x8e, 0x43, 0x44, 0xc4, 0xde, 0xe9, 0xcb,
6      0x54, 0x7b, 0x94, 0x32, 0xa6, 0xc2, 0x23, 0x3d,
7      0xee, 0x4c, 0x95, 0x0b, 0x42, 0xfa, 0xc3, 0x4e,
8      0x08, 0x2e, 0xa1, 0x66, 0x28, 0xd9, 0x24, 0xb2,
9      0x76, 0x5b, 0xa2, 0x49, 0x6d, 0x8b, 0xd1, 0x25,
10     0x72, 0xf8, 0xf6, 0x64, 0x86, 0x68, 0x98, 0x16,
11     0xd4, 0xa4, 0x5c, 0xcc, 0x5d, 0x65, 0xb6, 0x92,
12     0x6c, 0x70, 0x48, 0x50, 0xfd, 0xed, 0xb9, 0xda,
13     0x5e, 0x15, 0x46, 0x57, 0xa7, 0x8d, 0x9d, 0x84,
14     0x90, 0xd8, 0xab, 0x00, 0x8c, 0xbc, 0xd3, 0x0a,
15     0xf7, 0xe4, 0x58, 0x05, 0xb8, 0xb3, 0x45, 0x06,
16     0xd0, 0x2c, 0x1e, 0x8f, 0xca, 0x3f, 0x0f, 0x02,
17     0xc1, 0xaf, 0xbd, 0x03, 0x01, 0x13, 0x8a, 0x6b,
18     0x3a, 0x91, 0x11, 0x41, 0x4f, 0x67, 0xdc, 0xea,
19     0x97, 0xf2, 0xcf, 0xce, 0xf0, 0xb4, 0xe6, 0x73,
20     0x96, 0xac, 0x74, 0x22, 0xe7, 0xad, 0x35, 0x85,
21     0xe2, 0xf9, 0x37, 0xe8, 0x1c, 0x75, 0xdf, 0x6e,
22     0x47, 0xf1, 0x1a, 0x71, 0x1d, 0x29, 0xc5, 0x89,
23     0x6f, 0xb7, 0x62, 0x0e, 0xaa, 0x18, 0xbe, 0x1b,
24     0xfc, 0x56, 0x3e, 0x4b, 0xc6, 0xd2, 0x79, 0x20,
25     0x9a, 0xdb, 0xc0, 0xfe, 0x78, 0xcd, 0x5a, 0xf4,
26     0x1f, 0xdd, 0xa8, 0x33, 0x88, 0x07, 0xc7, 0x31,
27     0xb1, 0x12, 0x10, 0x59, 0x27, 0x80, 0xec, 0x5f,
28     0x60, 0x51, 0x7f, 0xa9, 0x19, 0xb5, 0x4a, 0x0d,
29     0x2d, 0xe5, 0x7a, 0x9f, 0x93, 0xc9, 0x9c, 0xef,
30     0xa0, 0xe0, 0x3b, 0x4d, 0xae, 0x2a, 0xf5, 0xb0,
31     0xc8, 0xeb, 0xbb, 0x3c, 0x83, 0x53, 0x99, 0x61,
32     0x17, 0x2b, 0x04, 0x7e, 0xba, 0x77, 0xd6, 0x26,
33     0xe1, 0x69, 0x14, 0x63, 0x55, 0x21, 0x0c, 0x7d
34 };

```