4-21-2014

A Simplified AES with Field Characteristic 7

Suzanne Craig
College of Arts and Sciences, Boise State University

A Novel Version of Simplified Rijndael Cryptosystem

Suzanne Craig

Boise State University

Boise State Undergraduate Research Conference
April 2014

Outline

Section 1

Mathematical Background

Mathematical Background

Definition

A structure formed by the set $\mathbb{F}$ with two operations, called multiplication, $\times$, and addition, $+$, is a **field** *if and only if $(\mathbb{F}, +)$ is an Abelian group containing an identity element called e, $(\mathbb{F}/\{e\}, \times)$ is an Abelian group and the law of distributivity applies to $\times$ over $+$.*

Theorem

All Galois Fields have order p^r where p is prime.

Mathematical Background

Definition

A **commutative ring** *is a set with two operations, called multiplication and addition. The set and operators must be such that: the set on addition is an abelian group, multiplication must be associative and commutative, multiplication is distributive over addition and it is commutative over the set.*

- When the elements of the set are polynomials of maximum degree n, it is called a polynomial ring.
- Example: Consider $GF(2^8)[x]$ and $f(x) = x^6 + x^3 + x + 1$. We can rewrite $f(x)$ as 01001011.

Advanced Encryption Standard

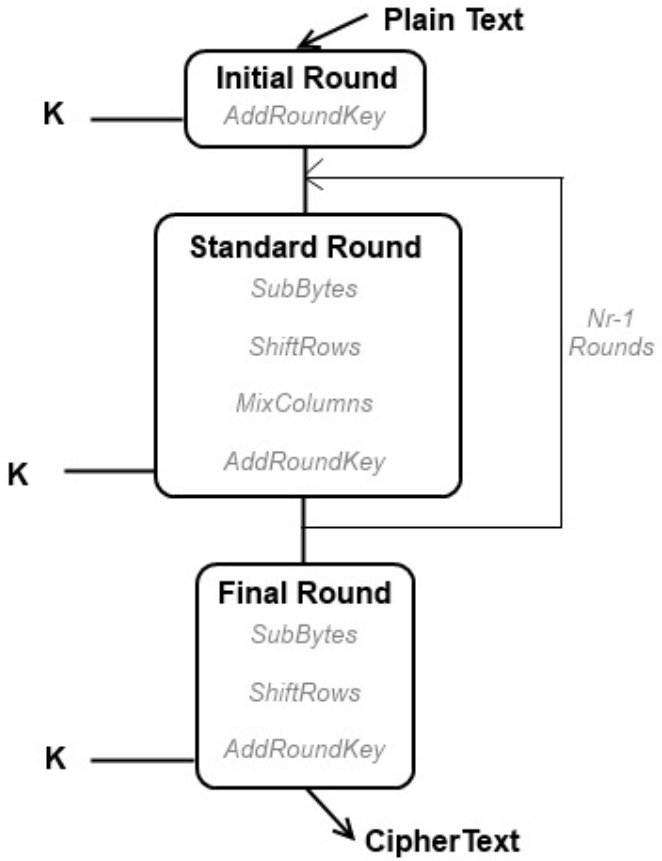

Figure: AES Structure

Basic Standards

- Ring: $GF(2^8)[x]$
- Irreducible Polynomial: $x^8 + x^4 + x^3 + x + 1$
- Block Size: 128 bits
- Key Size: 128, 192 or 256 bits

Simplified AES

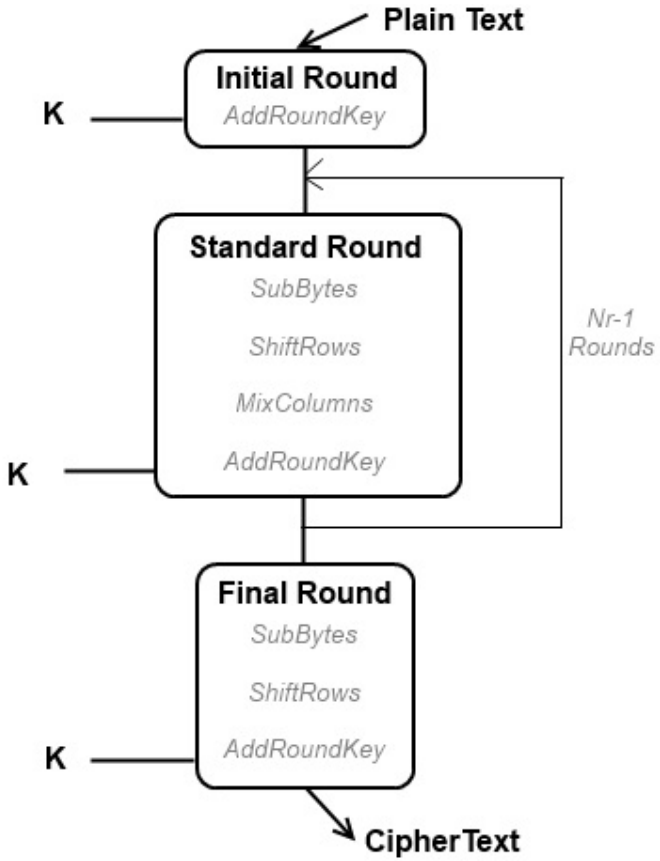

Figure: AES Structure.

Basic Standards

- Field: $GF(7^5)[x]$
- Irreducible Polynomial: $x^5 + 4x + 1$
- Block Size: 80 rits
- Key Size: 17 rits

Simplified AES

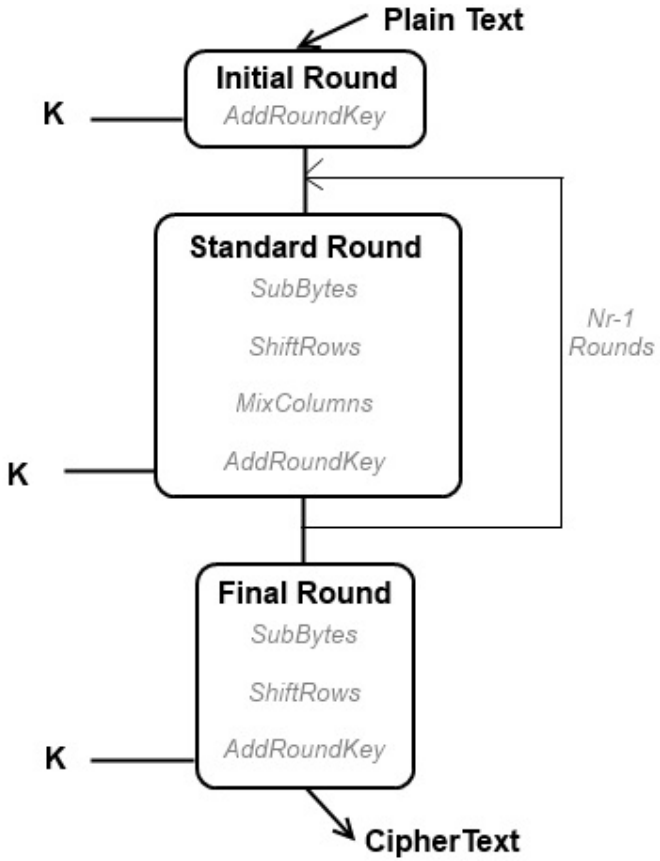

Figure: AES Structure.

Basic Standards

- Field: $GF(7^5)[x]$
- Irreducible Polynomial: $x^5 + 4x + 1$
- Block Size: 80 rits
- Key Size: 17 rits

So, what's a rit?

Simplified AES

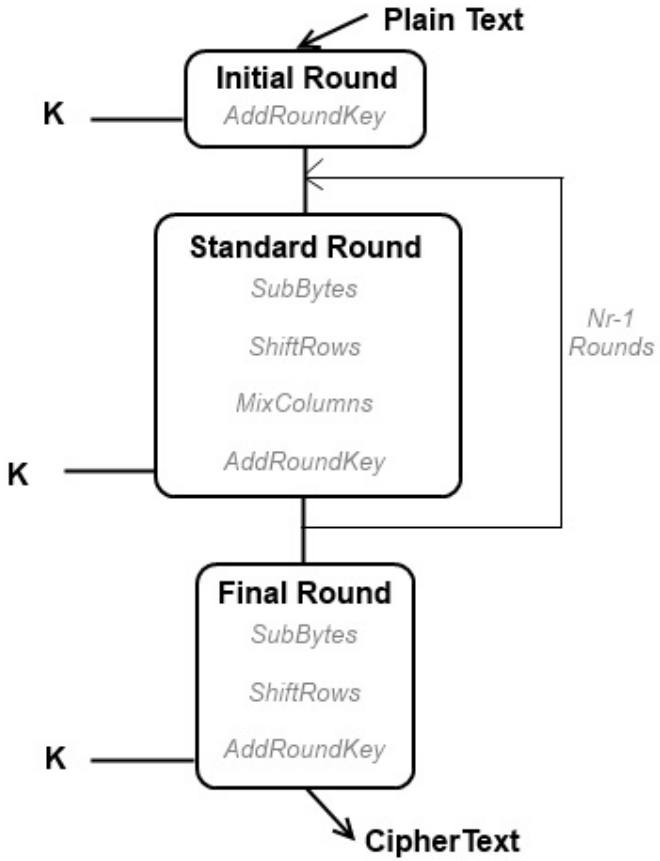

Figure: AES Structure.

Basic Standards

- Field: $GF(7^5)[x]$
- Irreducible Polynomial: $x^5 + 4x + 1$
- Block Size: 80 rits
- Key Size: 17 rits

So, what's a rit?

And why those sizes?

Section 2

Developing the Cryptosystem

Choosing the Field

Corollary 34

Let $p > 2$ be a prime. Then the set of s-round Rijndael-like functions do not form a group if

1. *s is even and ρ is odd, or else*
2. *s is odd and either π or λ is odd*

[1] Babinkostova, et. al, *Algebraic properties of generalized Rijndael-like ciphers*, **Groups Complexity Cryptology**, 2013.

Choosing the Field

Corollary 34

Let $p > 2$ be a prime. Then the set of s-round Rijndael-like functions do not form a group if

1. *s is even and ρ is odd, or else*
2. *s is odd and either π or λ is odd*

Lemma 17

Let $p > 2$ be prime. The function π is an odd perumutation if, and only if, $p \equiv_4 3$, n is even, r is odd, and $gcd(n, c(i))$ is odd for an odd number of $i \in \{0, ..., m-1\}$

1

[1] Babinkostova, et. al, *Algebraic properties of generalized Rijndael-like ciphers*, **Groups Complexity Cryptology**, 2013.

Choosing the Field cont.

- p: Chosen to be 7
  - Characteristic
- n: Chosen to be 4
  - Input Matrix Size
- r: Chosen to be 5
  - Exponent

SubByte Operation (λ)

Written as a matrix operation.

$$y = Ax^{-1} + B \tag{1}$$

SubByte Operation (λ)

Written as a matrix operation.

$$y = Ax^{-1} + B \tag{1}$$

A is a circulant, invertible matrix with elements in $\mathbb{Z}_7$

$$A = \begin{bmatrix} 0 & 0 & 2 & 5 & 1 \\ 1 & 0 & 0 & 2 & 5 \\ 5 & 1 & 0 & 0 & 2 \\ 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 5 & 1 & 0 \end{bmatrix} \tag{2}$$

SubByte Operation (λ)

Written as a matrix operation.

$$y = Ax^{-1} + B \tag{1}$$

A is a circulant, invertible matrix with elements in $\mathbb{Z}_7$

$$A = \begin{bmatrix} 0 & 0 & 2 & 5 & 1 \\ 1 & 0 & 0 & 2 & 5 \\ 5 & 1 & 0 & 0 & 2 \\ 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 5 & 1 & 0 \end{bmatrix} \tag{2}$$

x^{-1} is the inverse of the polynomial input in $GF(7^5)[x]$

SubByte Operation (λ)

Written as a matrix operation.

$$y = Ax^{-1} + B \tag{1}$$

A is a circulant, invertible matrix with elements in $\mathbb{Z}_7$

$$A = \begin{bmatrix} 0 & 0 & 2 & 5 & 1 \\ 1 & 0 & 0 & 2 & 5 \\ 5 & 1 & 0 & 0 & 2 \\ 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 5 & 1 & 0 \end{bmatrix} \tag{2}$$

x^{-1} is the inverse of the polynomial input in $GF(7^5)[x]$

B is a 5 element column vector. We chose the zero vector for simplicity.

MixColumn Operation (ρ)

Needs a circulant, invertible matrix, called C.

MixColumn Operation (ρ)

Needs a circulant, invertible matrix, called C.

In original AES, C is also an MDS matrix. $p = 3$ didn't give any 4×4 MDS matrices, but $p = 7$ did.

MixColumn Operation (ρ)

Needs a circulant, invertible matrix, called C.

In original AES, C is also an MDS matrix. $p = 3$ didn't give any 4×4 MDS matrices, but $p = 7$ did.

$$C = \begin{bmatrix} 0 & 1 & 1 & 3 \\ 3 & 0 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 1 & 3 & 0 \end{bmatrix} \tag{3}$$

MixColumn Operation (ρ)

Needs a circulant, invertible matrix, called C.

In original AES, C is also an MDS matrix. $p = 3$ didn't give any 4×4 MDS matrices, but $p = 7$ did.

$$C = \begin{bmatrix} 0 & 1 & 1 & 3 \\ 3 & 0 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 1 & 3 & 0 \end{bmatrix} \tag{3}$$

Input is whole block, but only one column is operated on at a time.

AddRoundKey ($\sigma[k]$) and ShiftRow (π)

AddRoundKey takes a 16 element subkey and arranges it in a 4×4 matrix. Then it is added to the input block in a rit-wise operation.

AddRoundKey ($\sigma[k]$) and ShiftRow (π)

AddRoundKey takes a 16 element subkey and arranges it in a 4×4 matrix. Then it is added to the input block in a rit-wise operation.

ShiftRow takes the entire 4×4 block and shifts each row to the left with increasing offsets. The first row is left alone, the second is shifted by one, the third by two and the fourth by three.

Section 3

An Example

Plaintext

$$M = 012035461235102546123562015203516445315050310124115605451136461235461230205354 13$$

Plaintext

$$M = 01203546123510254612356201520351644531505031012411560545113646123546123020535413$$

$$\mathcal{M} = \begin{bmatrix} 01203 & 54612 & 35102 & 54612 \\ 35620 & 15203 & 51644 & 53150 \\ 50310 & 12411 & 56054 & 51136 \\ 46123 & 54612 & 30205 & 35413 \end{bmatrix} \tag{4}$$

Key and Subkeys

$$K = 0156452105343120 0 \tag{5}$$

$$k_1 = 5645210534312000 \tag{6}$$

$$k_2 = 6452105343120001 \tag{7}$$

$$k_3 = 4521053431200015 \tag{8}$$

AddRoundKey

First, the subkey is written as a 4×4 matrix.

$$k_1 = \begin{bmatrix} 5 & 6 & 4 & 5 \\ 2 & 1 & 0 & 5 \\ 3 & 4 & 3 & 1 \\ 2 & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

AddRoundKey

First, the subkey is written as a 4×4 matrix.

$$k_1 = \begin{bmatrix} 5 & 6 & 4 & 5 \\ 2 & 1 & 0 & 5 \\ 3 & 4 & 3 & 1 \\ 2 & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

Then this is added to the plaintext matrix, rit-wise: $k_1 \oplus \mathcal{M}$

AddRoundKey

First, the subkey is written as a 4×4 matrix.

$$k_1 = \begin{bmatrix} 5 & 6 & 4 & 5 \\ 2 & 1 & 0 & 5 \\ 3 & 4 & 3 & 1 \\ 2 & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

Then this is added to the plaintext matrix, rit-wise: $k_1 \oplus \mathcal{M}$

$$State_1 = \sigma[k_1] = \begin{bmatrix} 56051 & 43501 & 02546 & 32460 \\ 50142 & 26314 & 51644 & 31635 \\ 13643 & 56155 & 12310 & 62240 \\ 61345 & 54612 & 30205 & 35413 \end{bmatrix} \tag{10}$$

SubByte

Element-wise operation. Using $State_1[1,1] = 56051$:

SubByte

Element-wise operation. Using $State_1[1,1] = 56051$:

Recall $56051 = 5x^4 + 6x^3 + 5x^2 + 1$.

SubByte

Element-wise operation. Using $State_1[1,1] = 56051$:

Recall $56051 = 5x^4 + 6x^3 + 5x^2 + 1$.

$$(56051)^{-1} \in GF(7^5)[x] = 3x^4 + 4x^3 + 5x^2 + x + 2 = 34512 \qquad (11)$$

SubByte

Element-wise operation. Using $State_1[1,1] = 56051$:

Recall $56051 = 5x^4 + 6x^3 + 5x^2 + 1$.

$$(56051)^{-1} \in GF(7^5)[x] = 3x^4 + 4x^3 + 5x^2 + x + 2 = 34512 \tag{11}$$

This is then written as a vector and multiplied by A.

$$\begin{bmatrix} 0 & 0 & 2 & 5 & 1 \\ 1 & 0 & 0 & 2 & 5 \\ 5 & 1 & 0 & 0 & 2 \\ 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 5 & 1 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \\ 1 \\ 2 \end{bmatrix} \mod 7 = \begin{bmatrix} 3 \\ 1 \\ 2 \\ 3 \\ 6 \end{bmatrix} \tag{12}$$

SubByte

Element-wise operation. Using $State_1[1,1] = 56051$:

Recall $56051 = 5x^4 + 6x^3 + 5x^2 + 1$.

$$(56051)^{-1} \in GF(7^5)[x] = 3x^4 + 4x^3 + 5x^2 + x + 2 = 34512 \tag{11}$$

This is then written as a vector and multiplied by A.

$$\begin{bmatrix} 0 & 0 & 2 & 5 & 1 \\ 1 & 0 & 0 & 2 & 5 \\ 5 & 1 & 0 & 0 & 2 \\ 2 & 5 & 1 & 0 & 0 \\ 0 & 2 & 5 & 1 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \\ 1 \\ 2 \end{bmatrix} \text{ mod } 7 = \begin{bmatrix} 3 \\ 1 \\ 2 \\ 3 \\ 6 \end{bmatrix} \tag{12}$$

$$\lambda(56051) = 31236 \tag{13}$$

SubByte

$$State_2 = \begin{bmatrix} 31236 & 42401 & 31643 & 26163 \\ 50355 & 33213 & 03400 & 20505 \\ 20244 & 55455 & 46500 & 02241 \\ 32315 & 15004 & 22153 & 25363 \end{bmatrix} \tag{14}$$

ShiftRow

$$State_3 = \pi(State_2) = \begin{bmatrix} 31236 & 42401 & 31643 & 26163 \\ 33213 & 03400 & 20505 & 50355 \\ 46500 & 02241 & 20244 & 55455 \\ 25363 & 32315 & 15004 & 22153 \end{bmatrix} \tag{15}$$

MixColumn

Using the first column of $State_3$:

$$\begin{bmatrix} 0 & 1 & 1 & 3 \\ 3 & 0 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 1 & 3 & 0 \end{bmatrix} \begin{bmatrix} 31236 \\ 33213 \\ 46500 \\ 25363 \end{bmatrix} = 0(31236) \oplus 1(33213) \oplus 1(46500) \oplus 3(25363) \tag{16}$$

$$= 0 \oplus 33213 \oplus 46500 \oplus 61242 = 63255 \tag{17}$$

This returns the first element of the first column. Each row in the C matrix returns the corresponding element in the column output.

MixColumn

Performing this operation on all four columns returns:

$$State_4 = \rho(State_3) = \begin{bmatrix} 63255 & 24102 & 01040 & 24345 \\ 10010 & 30356 & 51623 & 64103 \\ 01454 & 03662 & 36041 & 51450 \\ 41542 & 44054 & 41326 & 10252 \end{bmatrix} \tag{18}$$

Ciphertext

Performing the round functions in the order required by the AES encryption function with 1 intermediate round, we get:

$$\mathcal{C} = \begin{bmatrix} 10155 & 63014 & 33431 & 20544 \\ 11530 & 05461 & 33345 & 50516 \\ 33532 & 20212 & 52063 & 14524 \\ 63212 & 44645 & 22405 & 54363 \end{bmatrix} \tag{19}$$

Decryption

The decryption algorithm is the encryption algorithm backwards, with the round functions changed to produce their inverses.

Decryption

The decryption algorithm is the encryption algorithm backwards, with the round functions changed to produce their inverses.

InvSubByte requires an inverted A matrix in $\mathbb{Z}_7$, and rather than find the inverse of the input, you find the inverse of the output.

Decryption

The decryption algorithm is the encryption algorithm backwards, with the round functions changed to produce their inverses.

InvSubByte requires an inverted A matrix in $\mathbb{Z}_7$, and rather than find the inverse of the input, you find the inverse of the output.

InvShiftRow requires identical offsets for each row, but rather than shifting to the left you shift to the right.

Decryption

The decryption algorithm is the encryption algorithm backwards, with the round functions changed to produce their inverses.

InvSubByte requires an inverted A matrix in $\mathbb{Z}_7$, and rather than find the inverse of the input, you find the inverse of the output.

InvShiftRow requires identical offsets for each row, but rather than shifting to the left you shift to the right.

SubtractRoundKey means adding the additive inverse modulo 7 in a rit-wise operation.

Decryption

The decryption algorithm is the encryption algorithm backwards, with the round functions changed to produce their inverses.

InvSubByte requires an inverted A matrix in $\mathbb{Z}_7$, and rather than find the inverse of the input, you find the inverse of the output.

InvShiftRow requires identical offsets for each row, but rather than shifting to the left you shift to the right.

SubtractRoundKey means adding the additive inverse modulo 7 in a rit-wise operation.

InvMixColumn simply requires that the inverse C matrix in $\mathbb{Z}_7$ be used.

Decryption

$$A^{-1} = \begin{bmatrix} 4 & 6 & 4 & 5 & 3 \\ 3 & 4 & 6 & 4 & 5 \\ 5 & 3 & 4 & 6 & 4 \\ 4 & 5 & 3 & 4 & 6 \\ 6 & 4 & 5 & 3 & 4 \end{bmatrix} \tag{20}$$

$$C^{-1} = \begin{bmatrix} 5 & 5 & 1 & 6 \\ 6 & 5 & 5 & 1 \\ 1 & 6 & 5 & 5 \\ 5 & 1 & 6 & 5 \end{bmatrix} \tag{21}$$

Section 4

Results and Future Work

Results

Theorem

The simplified version of AES over the field $GF(7^5)$ is well-defined.

Conjecture

There are no MDS matrices of size greater than n in fields with characteristic n.

Future Work

- Work on conjectural result regarding MDS matrices.
- Conduct cryptanalysis on simplified AES to determine possible effects of increased characteristic.

Acknowledgements

- Boise State Department of Mathematics
- Boise State Honors College
- Boise State Student Research Initiative Program

And a special thanks to my faculty mentor, Liljana Babinkostova, PhD, and colleague David Albertson for assistance with Maple.

References I


C. Cid, S. Murphy and M.J.B. Robshaw.
"Small Scale Variants of the AES,"
Proceedings of Fast Software Encryption, Springer-Verlag, (2005).


K. Cartrysse and J.C.A van der Lubbe,
"The Advanced Encryption Standard: Rijndael,"
Basic Methods of Cryptography, Cambridge University Press (2004).


M. Musa, et. al.
"A Simplified AES Algorithm and its Linear and Differential Cryptanalysis,"
Cryptologia, Vol. 27, No. 2 (2003), pp. 148-177.
http://www.tandfonline.com/doi/pdf/10.1080/0161-110391891838


L. Babinkostova, et. al.,
"Algebraic properties of generalized Rijndael-like ciphers,"
Accessed 20 October 2013, `arXiv:1210.7942 [math.GR]`

Any Questions?