GENERATING THE AES S-BOX AND PERFORMING A LINEAR ANALYSIS

Presentation by Adam Hayse

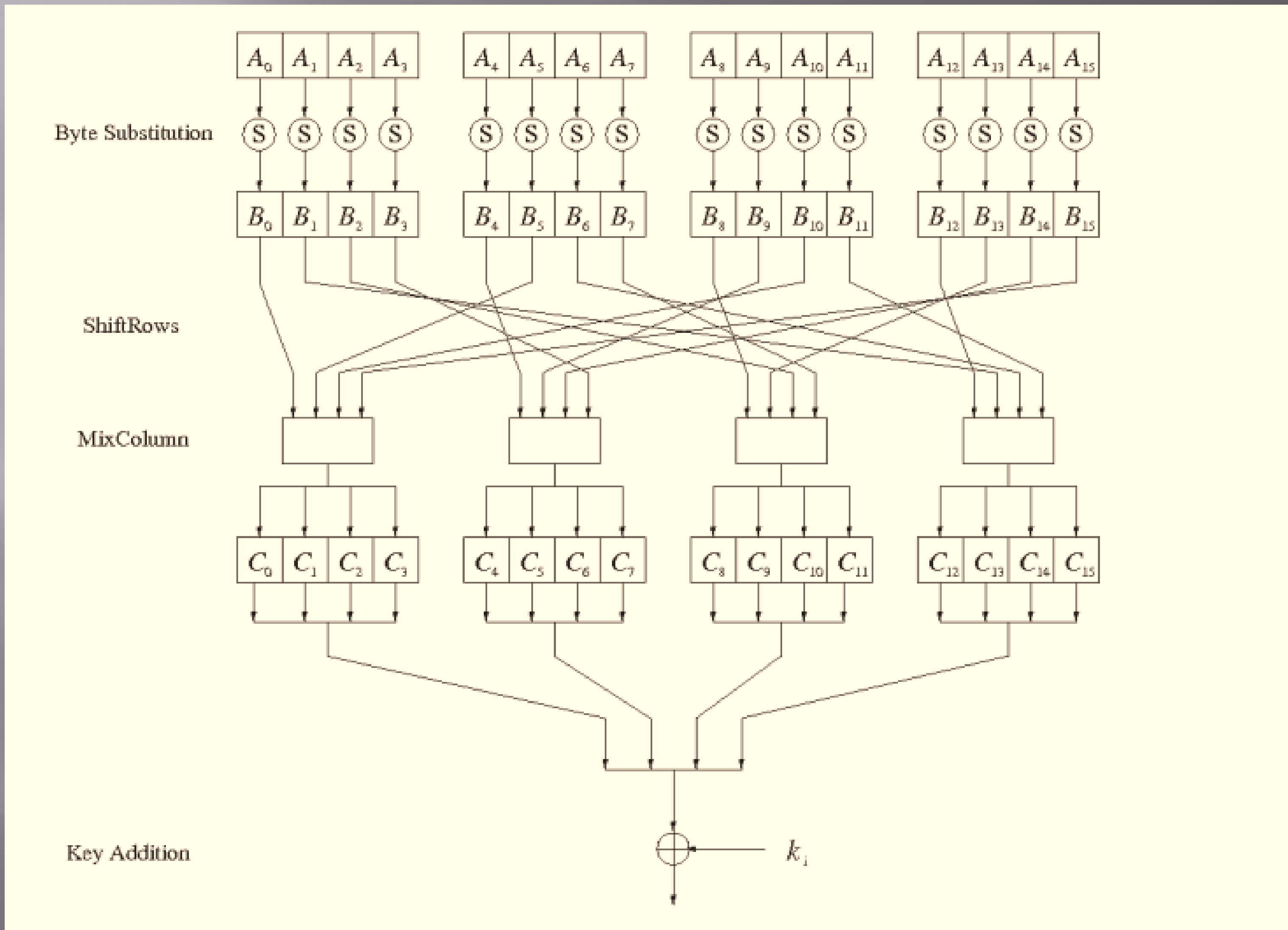
CS 492 – Computer Security

26 April 2017

Summary

- Advanced Encryption Standard (AES) Overview
- Define Finite Fields (Galois Fields)
- Arithmetic in Finite Fields
- Computing the Inverse by Hand
- Demonstration

128-bit AES Round Function



AES S-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	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Finite Fields

- A field is a set of elements for which the four basic operations are closed within the set
- Example: set of real numbers ($\mathbb{R}$)
- Given a, b $\in \mathbb{R}$:

$$a+b = c \in \mathbb{R}$$
$$a-b = c \in \mathbb{R}$$
$$a*b = c \in \mathbb{R}$$
$$a/b = c \in \mathbb{R}$$

- A finite field is a field that has a finite number of elements

Finite Fields

- A finite field only exists if its size is p^m, where p is a prime number and m is a natural number
- Two types of finite field:
  - Prime field (m=1)
  - Extension field (m>1)
- Need to map 8 bits to 8 bits, so we are interested in the finite field $GF(2^8)$.

Prime Field Arithmetic

- Addition: (a + b) mod p
- Subtraction: (a – b) mod p
- Multiplication: (a * b) mod p
- Division: $(a * b^{-1})$ mod p

- Example: $GF(5^1) = \{0, 1, 2, 3, 4\}$

Prime Field Arithmetic

- **Addition:**

	0	1	2	3	4
0	(0+0) mod 5	(0+1) mod 5	(0+2) mod 5	(0+3) mod 5	(0+4) mod 5
1		(1+1) mod 5	(1+2) mod 5	(1+3) mod 5	(1+4) mod 5
2			(2+2) mod 5	(2+3) mod 5	(2+4) mod 5
3				(3+3) mod 5	(3+4) mod 5
4					(4+4) mod 5

	0	1	2	3	4
0	0	1	2	3	4
1		2	3	4	0
2			4	0	1
3				1	2
4					3

- **Subtraction:**

	0	1	2	3	4
0	(0-0) mod 5	(0-1) mod 5	(0-2) mod 5	(0-3) mod 5	(0-4) mod 5
1	(1-0) mod 5	(1-1) mod 5	(1-2) mod 5	(1-3) mod 5	(1-4) mod 5
2	(2-0) mod 5	(2-1) mod 5	(2-2) mod 5	(2-3) mod 5	(2-4) mod 5
3	(3-0) mod 5	(3-1) mod 5	(3-2) mod 5	(3-3) mod 5	(3-4) mod 5
4	(4-0) mod 5	(4-1) mod 5	(4-2) mod 5	(4-3) mod 5	(4-4) mod 5

	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

- **Multiplication:**

	0	1	2	3	4
0					
1		(1*1) mod 5	(1*2) mod 5	(1*3) mod 5	(1*4) mod 5
2			(2*2) mod 5	(2*3) mod 5	(2*4) mod 5
3				(3*3) mod 5	(3*4) mod 5
4					(4*4) mod 5

	0	1	2	3	4
0					
1		1	2	3	4
2			4	1	3
3				4	2
4					1

Prime Field Arithmetic

1^{-1} mod 5: 1

2^{-1} mod 5:

$5 = 2(2) + 1$

$1 = 5(1) - 2(2)$

$1 = 5(1) + 2(-2)$

$-2 \bmod 5 = 3$

3^{-1} mod 5:

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$1 = 3(1) - 2(1)$

$1 = 3(1) - (5 - 3)(1)$

$1 = 3(2) - 5(1)$

$2 \bmod 5 = 2$

4^{-1} mod 5:

$5 = 4(1) + 1$

$1 = 5(1) - 4(1)$

$1 = 5(1) + 4(-1)$

$-1 \bmod 5 = 4$

	1^{-1}	2^{-1}	3^{-1}	4^{-1}
1	(1*1) mod 5	(1*3) mod 5	(1*2) mod 5	(1*4) mod 5
2		(2*3) mod 5	(2*2) mod 5	(2*4) mod 5
3			(3*2) mod 5	(3*4) mod 5
4				(4*4) mod 5

	1^{-1}	2^{-1}	3^{-1}	4^{-1}
1	1	3	2	4
2		1	4	3
3			1	2
4				1

Extension Field GF(2^m)

- The elements of GF(2^m) for m > 1 are polynomials of the form:

$$A(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

- The coefficients a_i of each polynomial belong to the sub-field GF(2^1) = {0, 1}, which is a prime field.

Example: GF(2^3)

- GF(8) = {0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1}

	x^2	x	1
0	0	0	0
1	0	0	1
x	0	1	0
x + 1	0	1	1
x^2	1	0	0
x^2 + 1	1	0	1
x^2 + x	1	1	0
x^2 + x + 1	1	1	1

Addition and Subtraction in GF(2^m)

$$A(x) = a_{m-1}x^{m-1} + \ \ldots + a_1x + a_0$$
$$B(x) = b_{m-1}x^{m-1} + \ \ldots + b_1x + a_0$$
$$A(x) \pm B(x) = \sum_{i=0}^{m-1} (ai \pm b_i \, mod \ 2)$$

Add:

$(x+1) + (x^2+x) = x^2 + (1+1)x + 1 = x^2 + 1$

011 + 110 = 101

Subtract:

$(x+1) - (x^2+x) = (0-1)x^2 + (1-1)x + (0-1)1 = x^2 + 1$

011 - 110 = 101

Multiplication in GF(2^m)

- If we try to simply multiply two polynomials in GF(8), we get something like this:

$$(x^2+1)(x^2+x) = x^4 + x^3 + x^2 + x$$

$$x^4 + x^3 + x^2 + x \notin GF(2^3)$$

- The result is not in the field.
- Need a polynomial that behaves like a prime number.

Irreducible Polynomials

- Irreducible polynomials cannot be factored
- The degree of the polynomial used in GF(2^m) must be of degree m
- There are usually many polynomials of degree m that fit these requirements
- AES uses GF(2^8) and the irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$
- The hexadecimal representation is 0x11b

Polynomial Modular Reduction

- A degree 3 irreducible polynomial is $x^3 + x + 1$

11110	$(x^4 + x^3 + x^2 + x) : (x^3 + x + 1) = x + 1$
1011	$+x^4 \quad +x^2 \quad +x$

01000	x^3
1011	$+x^3 \quad +x \quad +1$

0011	$x + 1$

Extended Euclidean Algorithm for Polynomials

- When applied to integers, the formula is:

$$a = bq + r, \text{ where } q \in \mathbf{Z} \text{ and } 0 \leq r < |b|$$

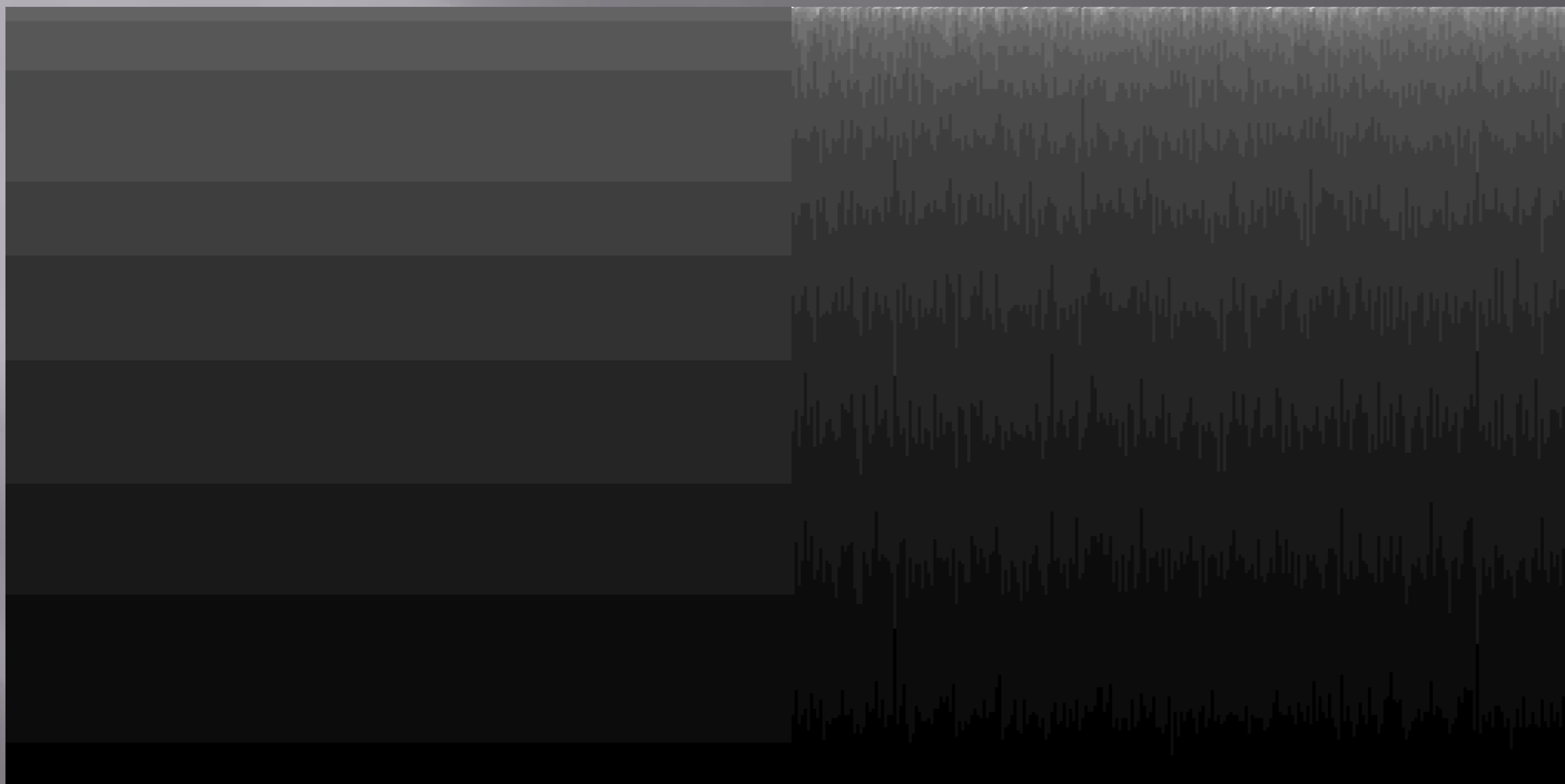
- When applied to polynomials, the formula is similar:

$$A(x) = B(x)Q(x) + R(x)$$

where $Q(x)$ is a polynomial such that

$$0 \leq \deg(R(x)) < \deg(B(x))$$

Linear Analysis



References

- Paar, Christof. "Advanced Encryption Standard (AES)." *YouTube*. Web. 26 Mar. 2017. <https://www.youtube.com/watch?v=NHuibtoL_qk>.
- Paar, Christof. "Introduction to Galois Fields for the AES." *YouTube*. Web. 26 Mar. 2017. <https://www.youtube.com/watch?v=x1v2tX4_dkQ>.
- Stamp, Mark. *Information security: principles and practice*. Hoboken, NJ: Wiley, 2011. Print.
- Daemen, Joan, and Vincent Rijmen. National Institute of Standards and Technology. N.p., 9 Mar. 1999. Web. 26 Mar. 2017. <http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf#page=1>