NORTHERN ARIZONA UNIVERSITY®

INF 638
Cryptography & Cryptosystems

Section 5: Advanced Encryption System

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

5-Advanced Encryption Standard

- 5-A Finite (Galois) fields
  - Definitions
  - Arithmetic of Prime Galois fields
  - Arithmetic of Extended Galois fields
- 5-B Advanced Encryption Standard

Properties in the group theory
Operations "$\oplus$" and "$\otimes$"

Associative: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

Commutative: $a \oplus b = b \oplus c$

Distributive: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

and $(a \oplus b) \otimes c = (a \otimes c) \oplus (a \otimes c)$

Zero for $\oplus$: $a \oplus 0 = 0 \oplus a = a$

Inverse for $\oplus$: $a \oplus -a = -a \oplus a = 0$

Subtraction : $a \ominus b = a \oplus -b$

One for $\otimes$: $a \otimes 1 = 1 \otimes a = a$

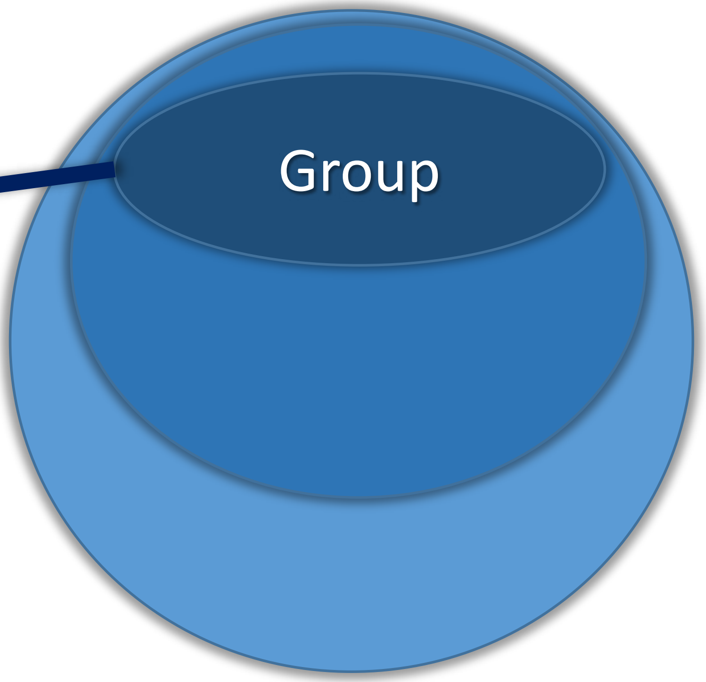
Inverse for $\otimes$: $a \otimes a^{-1} = a^{-1} \otimes a = 1$

Division : $a \oplus\!\!\!\!\div\, b = a \otimes b^{-1}$

Three basic algebraic structures

1- Group: Operations $\oplus$ & $\ominus$

- Closed
- Associative
- Abelian groups are commutative
- Have a neutral "0" $\quad a \oplus 0 = 0 \oplus a = a$
- All elements have an inverse $\quad a \oplus (-a) = (-a) \oplus a = 0$
- Subtraction: $\quad a \ominus b = a \oplus (-b)$



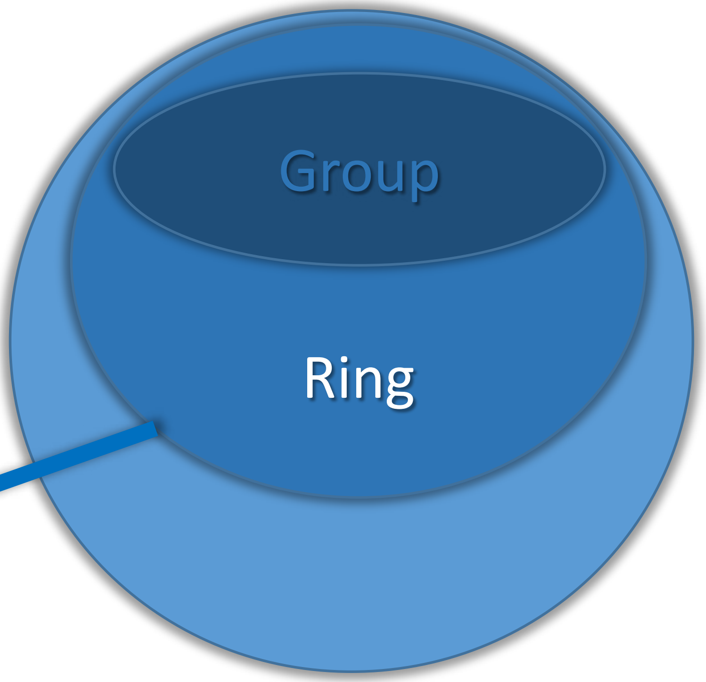
$\mathbb{R}$: Reals numbers are a group

$\mathbb{C}$: Complex numbers are a group

$\mathbb{Z}$: Integer numbers are a group

$\mathbb{N}$: Positive Integer numbers: no

Three basic algebraic structures



1- <u>Group</u>: Operations $\oplus$ & $\ominus$

2- <u>Ring:</u> Operations $\oplus$ $\ominus$ $\otimes$

$\oplus$ $\ominus$: Abelian group

$\otimes$: Closed

Associative

Neutral “1”: $1 \otimes a = a \otimes 1 = a$

$\oplus$ & $\otimes$: Distributive

$\mathbb{R}$: Reals numbers are a ring

$\mathbb{C}$: Complex numbers are a ring

$\mathbb{Z}$: Integer numbers are a ring

$\mathbb{N}$: Positive Integer numbers: no

Three basic algebraic structures

1- Group: One operation $\oplus$ $\ominus$

2- Ring: Operations $\oplus$ $\ominus$ $\otimes$

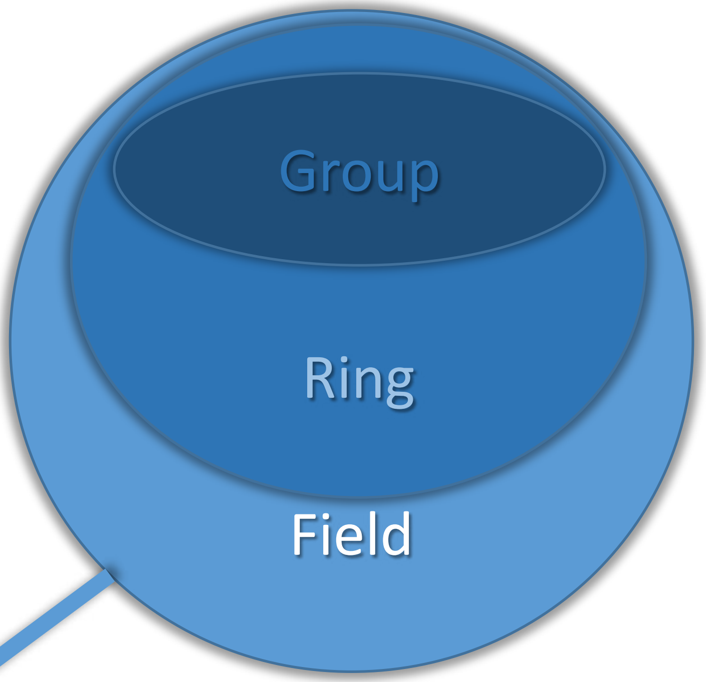
3- **Field:** Operations $\oplus$ $\ominus$ $\otimes$ $\oslash$

$\oplus$ $\ominus$ $\otimes$: Ring,

$\otimes$: Commutative

All elements but 0 have an inverse

$a \otimes a^{-1} = 1$ $\quad a^{-1} = 1/a$ $\quad a \oslash b = a \otimes (b^{-1})$



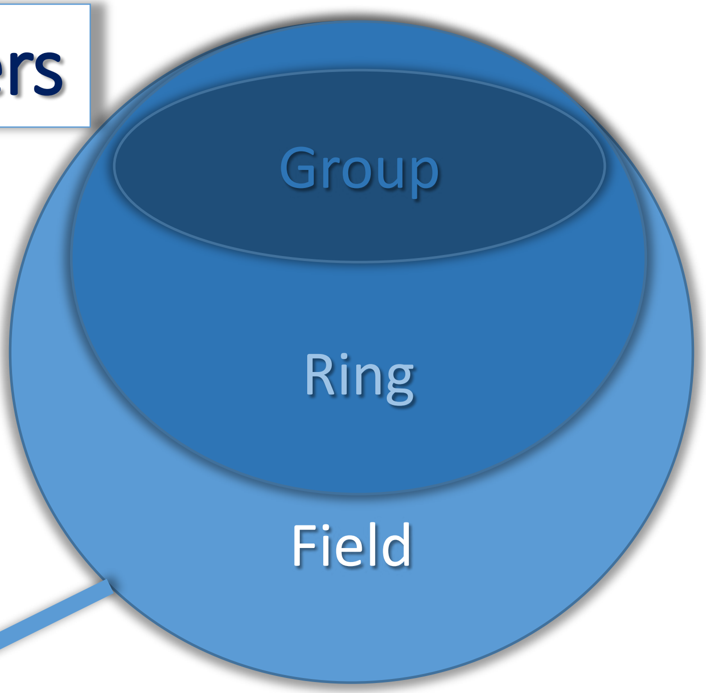
$\mathbb{R}$: Reals numbers are a field

$\mathbb{C}$: Complex numbers are a field

$\mathbb{Z}$: Integer numbers: no

$\mathbb{N}$: Positive Integer numbers: no

Finite fields are based on natural numbers



ℕ: Positive Integer numbers:

The Galois fields are fields with natural numbers

The arithmetic is different

5-Advanced Encryption Standard

- 5-A Galois fields
  - Definitions
  - Arithmetic of Prime Galois fields
  - Arithmetic of Extended Galois fields
- 5-B Advanced Encryption Standard

Definition prime Galois field and extension field

The Galois field $\mathcal{GF}_n$, $n \in \mathbb{N}$, is defined by the modulo of n:

$$\mathcal{GF}_n = \{0, 1, 2, \ldots, n-1\}$$

Only when $n = \mathbf{p}^m$, p is prime, $m \in \mathbb{N}$

Two cases:

1- Prime Galois field:

$\mathcal{GF}_p$ with p prime, $m = 1$

2- Extension of Galois Field:

$\mathcal{GF}_{p^m}$ with $\mathbf{p}^m$; p is prime ; m is integer

Examples of prime Galois field and extension field

$\mathcal{GF}_{11}$ is prime Galois field: has 11 elements

$\mathcal{GF}_{3^4}$ is extension Galois field: has 81 elements

$\mathcal{GF}_{12}$ is **not** a Galois field

$\mathcal{GF}_{2^8}$ is used for AES: has 256 elements

$\mathcal{GF}_{2^{256}}$ is used for Elliptic Curves (ECC)

The prime Galois fields (definitions 1-3)

1- The set of integers $\mathcal{GF}_p = \{0, 1, 2, \dots, p\text{-}1\}$

with the operations "$\oplus$" and "$\otimes$", p is prime

2- The two operations "$\oplus$" and "$\otimes$"

for all of a and $b \in \mathcal{GF}_p$ are "closed":

$$a \oplus b = c;\ \text{then } c \in \mathcal{GF}_p$$

$$a \otimes b = d;\ \text{then } d \in \mathcal{GF}_p$$

3- Associativity for all of $a, b, c \in \mathcal{GF}_p$:

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

The Galois fields (definitions 4-6)

4- There is a "0" for "$\oplus$", and "1" for "$\otimes$" for all elements a of $\mathcal{GF}_p$:

$a \oplus 0 = a$ $\quad$ $a \otimes 1 = a$ $\quad$ (0 and 1 are neutral)

5- The inverse exist for $\oplus$ such as: $\quad a \oplus (-a) = 0$

6- The inverse exist for $\otimes$ within $\mathcal{GF}_p$: $\quad a \otimes \boldsymbol{a}^{-1} = 1$

(not for the 0)

Arithmetic of the prime Galois fields

1- The set of integers $G\mathcal{F}_p = \{0, 1, 2, \ldots, p\text{-}1\}$; p is prime

2- **Addition**, **subtraction**, **multiplication**

$$c = a \oplus b = a + b \bmod p$$

$$d = a \ominus b = a - b \bmod p$$

$$e = a \otimes b = a.\, b \bmod p$$

3- **Inverse** and **division**

$$a \otimes \boldsymbol{a}^{-1} \equiv 1 \bmod p$$

(how to resolve this will be presented section 1-2 with EEA)

$$a \oplus\!\!\!\!\div\, b \equiv a\,.\,\boldsymbol{b}^{-1} \bmod p$$

Examples in the prime Galois fields

1- Example prime field: $\mathcal{GF}_5 = \{0, 1, 2, 3, 4\}$ is described by the following tables

$\oplus$	0	1	2	3	4	inverse
0	0	**1**	2	3	4	0
1	**1**	2	3	4	0	4
2	2	3	4	0	**1**	3
3	3	4	0	**1**	2	2
4	4	0	**1**	2	3	1

$\otimes$	0	1	2	3	4	inverse
0	0	0	0	0	0	NA
1	0	**1**	2	3	4	1
2	0	2	4	**1**	3	3
3	0	3	**1**	4	2	2
4	0	4	3	2	**1**	4

4/3 = 4x2 ≡ **3** mod5 ; **3/4** = 3x4≡ **2** mod5

1/(3/4) =1/2= **3** ≡ **4/3** mod5

4/2 = 4x3≡ **2** mod5 ; **2/4** = 2x4≡ **3** mod5

1/(4/2) =1/2= **3** ≡ **2/4** mod5

2- Example prime field: $\mathcal{GF}_2 = \{0, 1\}$ is described by the following tables

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Examples in the prime Galois fields: p=19

$G\mathcal{F}_{19} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$

$\otimes$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	17	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	17	6	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

a	inv
1	1
2	10
3	13
4	5
5	4
6	16
7	11
8	12
9	17
10	2
11	7
12	8
13	3
14	15
15	14
16	6
17	9
18	18

Homework: prime Galois fields with p=19

$\mathcal{GF}_{19} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$

A- 8/4
4/8
1/(8/4)

B- 12/3
3/12
1/(3/12)

C- 14/7
7/14
1/(7/14)

D- 9/3
3/9
1/(3/9)

E- 15/5
5/15
1/(5/15)

F- 15/3
3/15
1/(3/15)

G- 10/5
5/10
1/(5/10)

H- 18/3
3/18
1/(3/18)

I- 16/4
4/16
1/(4/16)

5-Advanced Encryption Standard

- 5-A Galois fields
  - Definitions
  - Arithmetic of Prime Galois fields
  - Arithmetic of Extended Galois fields
- 5-B Advanced Encryption Standard

Extension Fields $\mathcal{GF}_{2^8}$ (definition 1)

In AES the finite field contain 256 elements and is noted $\mathcal{GF}_{2^8}$

1- In the extended field the elements $A \in \mathcal{GF}_{2^8}$ are represented by polynomials:

$$A_{(x)} = a_7\, x^7 + \ldots + a_i\, x^i + \ldots + a_1\, x^1 + a_0; \;\; a_i \in \mathcal{GF}_2 = \{0, 1\}$$

This polynomials can be stored as:

$$A = (\, a_7\,, \ldots, a_i\,, \ldots, a_1, a_0)$$

Ex: $\mathcal{GF}_{2^3}$ elements are represented by polynomials: $A_{(x)} = a_2\, x^2 + a_1\, x^1 + a_0$

Binary	000	001	010	011	100	101	110	111
Polynomials	0	1	x	$x\ +1$	x^2	x^2+1	x^2+x	$x^2+x\ +1$

Extension Fields $\mathcal{GF}_{2^8}$ (definitions 2-3)

2- Addition in $\mathcal{GF}_{2^8}$ with $A_{(x)}$, $B_{(x)}$, $C_{(x)}$ ϵ $\mathcal{GF}_{2^8}$

$$C_{(x)} = A_{(x)} \oplus B_{(x)} = \sum_0^7 c_i\, x^i \quad ; \; c_i \equiv a_i + b_i \bmod 2$$ (it is a XOR)

3- Subtraction in $\mathcal{GF}_{2^8}$ with $A_{(x)}$, $B_{(x)}$, $C_{(x)}$ ϵ $\mathcal{GF}_{2^8}$

$$C_{(x)} = A_{(x)} \ominus B_{(x)} = \sum_0^7 c_i\, x^i \quad ; \; c_i \equiv a_i - b_i \bmod 2$$

However: $a_i + b_i \bmod 2 = a_i - b_i \bmod 2 = c_i$

As a result $A_{(x)} \oplus B_{(x)} = A_{(x)} \ominus B_{(x)}$

[both addition and subtraction are commutative]

Example Extension Fields $\mathcal{GF}_{2^3}$

$$A_{(x)} = x^2 + x + 1 \quad (1\ 1\ 1)$$

$$B_{(x)} = x^2 + 1 \quad (1\ 0\ 1)$$

$$A_{(x)} + B_{(x)} = x \quad (0\ 1\ 0)$$

Extension Fields $\mathcal{GF}_{2^8}$ (definitions 4-6)

4- **Multiplication** in $\mathcal{GF}_{2^8}$ with $A_{(x)}, B_{(x)}, C_{(x)} \in \mathcal{GF}_{2^8}$

$$C_{(x)} = A_{(x)} \otimes B_{(x)} \equiv A_{(x)} \cdot B_{(x)} \mod P_{(x)}$$

With $P_{(x)}$ the irreducible polynomial: $P_{(x)} = x^8 + x^4 + x^3 + x + 1$

This polynomial is arbitrary, and part of AES standard

5- **Inverse** $A_{(x)} \otimes A^{-1}_{(x)} \equiv 1. \mod P_{(x)}$ (extended Euclidian Alg.)

6- **Division** $C_{(x)} = A_{(x)} \oplus B_{(x)} \equiv A_{(x)} \cdot B^{-1}_{(x)} \mod P_{(x)}$

For $\mathcal{GF}_{2^3}$ the irreducible polynomial can be $P_{(x)} = x^3 + x + 1$

Example: Extension Fields $\mathcal{GF}_{2^3}$

Irreducible polynomial (arbitrary): $P_{(x)} = x^3 + x + 1$

Example: A(1 1 1) x B(1 0 1) = ???

$$A_{(x)} = x^2 + x + 1 \quad ; \quad B_{(x)} = x^2 + 1$$

$$A_{(x)} \cdot B_{(x)} = (x^2 + x + 1) \cdot (x^2 + 1)$$

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

$$= x^4 + x^3 + x + 1 = CA_{(x)}$$

$$CA_{(x)} \equiv C_{(x)} \bmod P_{(x)}$$

We need to divide $CA_{(x)}$ *by* $P_{(x)}$, and find the reminder $C_{(x)}$

Example: Extension Fields $\mathcal{GF}_{2^3}$

$$x^4 + x^3 + x + 1 : x^3 + x + 1 = ?$$

$$
\begin{array}{lllll}
 & x^4 + x^3 + x + 1 & \Leftarrow & x^4 + x^3 + x + 1 = CA_{(x)} & \\
- & x^4 + x^2 + x & \Leftarrow & x \,.\, (x^3 + x + 1) = x \,.\, P_{(x)} & \\
= & x^3 + x^2 + 1 & & & \\
- & x^3 + x + 1 & \Leftarrow & 1 \,.\, (x^3 + x + 1) = 1 \,.\, P_{(x)} & \\
= & x^2 + x & \Leftarrow & C_{(x)} & \text{Reminder}
\end{array}
$$

$$C_{(x)} = (1\ 1\ 0)$$

$$x^4 + x^3 + x + 1 = (x^3 + x + 1)(x + 1) + (x^2 + x) \rightarrow C'_{(x)} \equiv \overbrace{(x^2 + x)} \mod (P_{(x)})$$

$$\boxed{(1\ 1\ 1) \times (1\ 0\ 1) = (1\ 1\ 0)}$$

Homework: find the Inverses in $\mathcal{GF}_{2^3}$?

Ex: $\mathcal{GF}_{2^3}$ are represented by polynomials: $A_{(x)} = a_2 x^2 + a_1 x^1 + a_0$

Elements: $(0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1)$

$$A_{(x)} \otimes A^{-1}_{(x)} \equiv 1.\ mod\ P_{(x)}$$

Multiply	000	001	010	011	100	101	110	110
000 (0)								
001 (1)								
010 (x)								
011 (x +1)								
100 (x^2)								
101 (x^2 + 1)								
110 (x^2+ x)								
111 (x^2+ x +1)								

$A_{(x)}$	$A^{-1}_{(x)}$
000	
001	
010	
011	
100	
101	
110	
111	

Inverse in $\mathcal{GF}_{2^8}$

$$A_{(x)} = a_7 x^7 + \ldots + a_i x^i + \ldots + a_1 x^1 + a_0$$

$$A_{(x)} \otimes A^{-1}_{(x)} \equiv 1 \bmod P_{(x)}$$

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

Example:

1101 0001 (i.e d1)

Inverse

0000 0111 (i.e 07)

$a_S = (a_3, a_2, a_1, a_0)$

$a_L = (a_7, a_6, a_5, a_4)$

$a_L \backslash a_S$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3
f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c

5-Advanced Encryption Standard

- 5-A Galois fields
  - Definitions
  - Arithmetic of Prime Galois fields
  - Arithmetic of Extended Galois fields
- 5-B Advanced Encryption Standard

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu