Basic Number Theory & Advanced Encryption Standard (AES)

KEPAL - Keamanan Perangkat Lunak

Minggu 04 Sesi 01

Togu Novriansyah Turnip, S.S.T., M.I.M.

Diploma III Teknologi Informasi

AGENDA

1. Mathematical Backgrounds: Basic Concept of Number Theory
2. AES
   - A. Subbytes
   - B. Shiftrows
   - C. Mixcolumns
   - D. Addroundkey

Mathematical Backgrounds

1

Group, Ring, Field, Modular Arithmetic, XOR and mod Operation.

Introduction

- of increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- concern operations on “numbers”
  - where what constitutes a “number” and the type of operations varies considerably
- start with concepts of groups, rings, fields from abstract algebra

Definition of "group"

- A group G, denoted by $\{G, \bullet\}$ is a set of elements with a binary operation $\bullet$, that associates to each ordered pair (a, b) of elements in G an element $(a \bullet b)$ in G, such that the following axioms are obeyed:
  - (A1) **Closure** : If a and b belong to G, then a•b is also in G
  - (A2) **Associative** : a•(b•c) = (a•b) •c for all a, b, c in G
  - (A3) **Identity element** : There is an element e in G such that a•e = e•a = a for all a in G
  - (A4) **Inverse element** : For each a in G, there is an element a^{-1} in G, such that $a \bullet a^{-1} = a^{-1} \bullet a = e$
  - **NB**: • could be addition +, multiplication x or any other mathematical operator

Definition of "group"

- A group has a finite number of elements is called finite group, and the order of the group is equal to the number of elements in the group. Otherwise the group is an **infinite group**
- A group is an abelian group if it satisfies the following additional condition:
  - (A5) **Commutative**: a•b = b•a for all a, b in G
- Suppose that exponentiation is defined within a group G, i.e., a^n = a•a•...•a (for n times) and a^0 = e. We say that G is **cyclic** if every element of G is a power a^k (for some k) of a fixed element a in G, where a is called a **generator** of G

Definition of Ring

- A ring R, defined by $\{R, +, \mathbf{x}\}$, is a set of elements with two binary operations, called ***addition*** and ***multiplication***, such that for all a, b, c in R the following axioms are obeyed:
- (A1~A5) R is an abelian group with respect to addition. For the case of an additive group, the identity element is 0 and the inverse of a is $-a$
- (M1) Closure under multiplication: if a, b in R, then ab also in R
- (M2) Associative of multiplication: $a(bc) = (ab)c$
- (M3) Distributive laws: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$

Definition of Ring

- A ring **R** is said to be **commutative** if the following axioms are obeyed:
  - (M4) Commutative of multiplication: $ab = ba$ for all a, b in R
- An **integral domain** is a commutative ring that satisfies the following axioms:
  - (M5) Multiplicative identity: There is an element 1 in R, such that a1 = 1a = a
  - (M6) No zero divisor: If a, b in R, and ab = 0 then, either $a = 0$ or $b = 0$

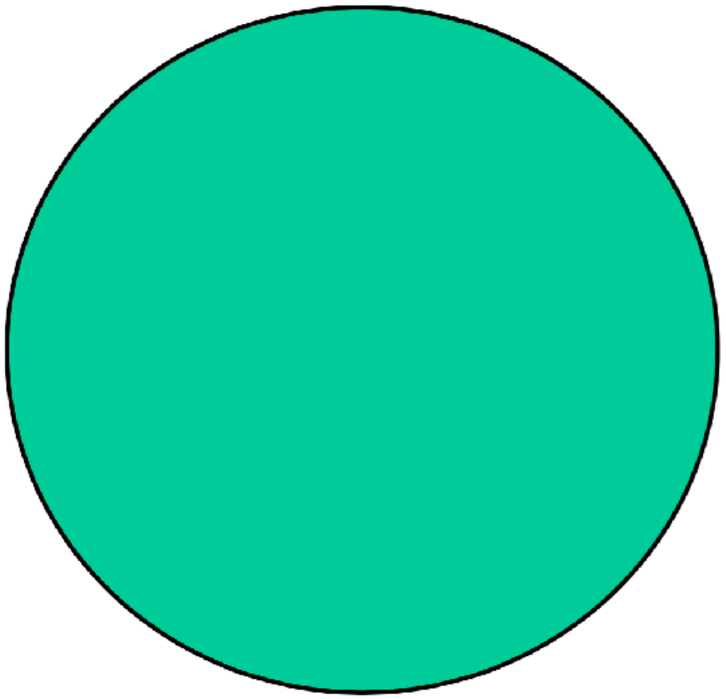
.

Definition of "field"

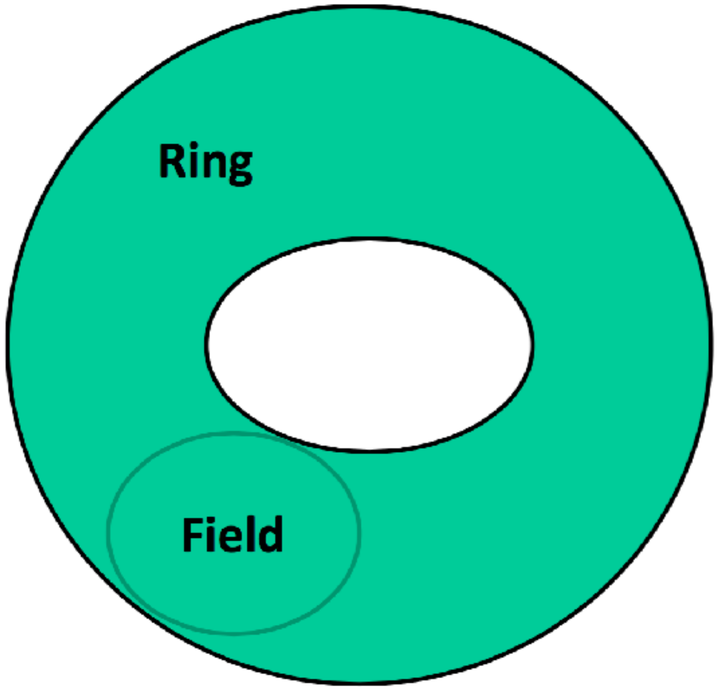
- A field $\mathbf{F}$, defined by $\{\mathbf{F}, +, \mathbf{x}\}$, is a set of elements with two binary operations, called **addition** and **multiplication**, such that for all a, b, c in R the following axioms are obeyed:
- (A1~M6)F is an integral domain
- (M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F, such that $a \cdot a^{-1} = a^{-1}a = 1$
- Note that **division** is defined as $\frac{a}{b} = a(b^{-1})$, for $b \neq 0$
- For a given prime p, a special finite field of order p is denoted by *GF*(*p*), *GF* means Galois field, in honor of the mathematician who first studied finite field.

A Finite Group, Ring, and Field

A finite group



Ring and Field



***Contoh Aplikasi Group, Ring, dan Field**

Modular Arithmetic

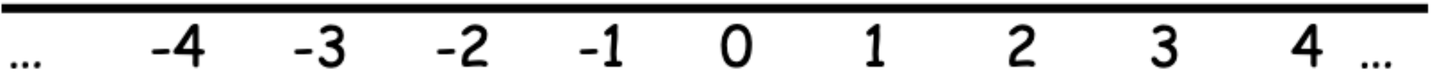
- '**clock arithmetic**'
- Uses a finite number of values, and loops back from either end.
- Modular arithmetic is when do addition & multiplication and modulo reduce answer
- Can do reduction at any point, ie
  - **a+b mod n = [a mod n + b mod n] mod n**
- When reducing, we "usually" want to find the positive remainder which is the normal reminder after dividing by the modulus.

Modular Arithmetic

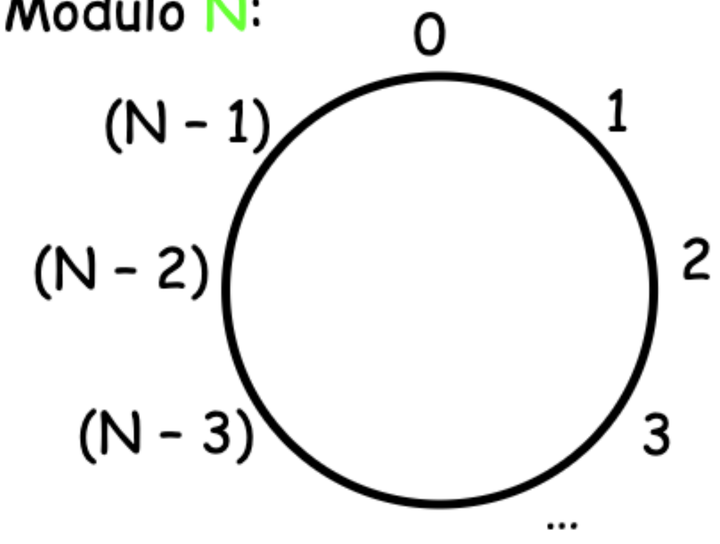
- can do modular arithmetic with any group of integers: $Z_n = \{0, 1, \ldots, n-1\}$
- Z_n represents a residue class.
- A commutative ring with a multiplicative identity element.
- Note some peculiarities:
  - **if** $(a + b) \equiv (a + c) \bmod n$ **then** $b \equiv c \bmod$
  - but, $(ab) \equiv (ac) \bmod n$ then $b \equiv c \bmod n$ only if a is **relatively prime** to n.

Modulo 8 Addition Example

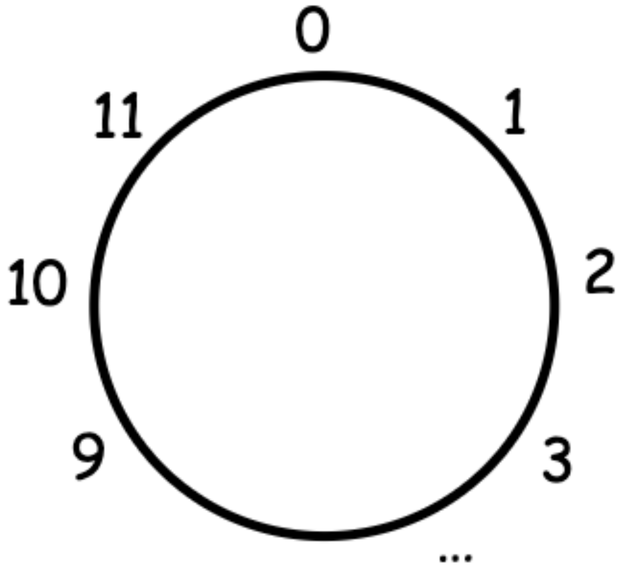
- Ordinary integers:



- Integers Modulo N:



- Example: Arithmetic Modulo 12
  (like Arithmetic on time)
- 3 + 11 (Modulo 12) = 2
- 2 – 4 (Modulo 12) = 10
- 5 * 4 (Modulo 12) = 8
- 4 * 3 (Modulo 12) = 0



Modulo 8 Addition Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Important properties of group and field in cryptography

- Most of cryptographic operations (arithmetic or logic computation) are in a “finite” domain with closure and inverse properties
- Let Enc be the encryption function and Dec be the decryption function of a crypto algorithm
  - If $C = Enc(K, M)$ and $M = Dec(K, C)$, then the crypto algorithm is **symmetric**
  - If $C = Enc(K, M)$ and $M = Dec(K^{-1}, C)$, then the crypto algorithm is **asymmetric**

Encryption Methods

Substitution Cipher

- In such cipher, one unit of ciphertext is **substituted** for a corresponding unit of plaintext
- For example, ABCD→BODK

Transportation Cipher

- In such cipher, units of the original plaintext are simply **shuffled around.**
- For example,
  THIS IS A SECRET →
  TATHSIESCIRSE
  T H I S I S
  A S E C R E
  T

Development of Cryptography

Conventional Cipher

- Logic operation

$$C = M \oplus K \quad M = C \oplus K$$

- Arithmetic operation

$$C = M \times K \bmod P \qquad M = C \times K^{-1} \bmod P$$

- Substitution(Caesar Chiper)

A → C, B → D, C → E, D → F, …, Z → B

$f(x) = x + 3 \bmod 26$

$f(x) = ax + b \bmod N$

Modern Cipher

- Logic + Arithmetic + Substitution → permutation or combination
- Symmetric algorithm: DES, AES
- Asymmetric algorithm: RSA, ElGamal, ECC

Why use XOR Cipher?

- XOR property
  - $0 \oplus 0 = 0,\ 1 \oplus 1 = 0$
  - $0 \oplus 1 = 1,\ 1 \oplus 0 = 1$
  - Guessing the one-bit result is “0” or “1” is with the probability 1/2
- XOR operation can be completed in **a single logic step** (or implemented by basic logic gates)
- XOR cipher is **very easy to be implemented** in **hardware** or **software** approach

Why use "mod" Operation?

- $X = Y \bmod Z$
  - e.g., 3 = 13 mod 5, 3 = (-7) mod 5
  - All *Y*'s presented in the form *kZ* + *X*, for any integer *k*, have the same property in the same **class**
  - All arithmetic computation used in crypto algorithms is based on the principle of "**finite state machine**"
  - It can be used to avoid the "**overflow**" problem of computation with large integers (e.g., > 512 bits)
  - It can be used to keep the basic property of "**closure**" in "group", "ring" or "field"

Modern Data Encryption Algorithms

2

Advance Encryption Standard(AES) - NIST - 2001

The Rise of AES

- Computing power of attackers are **dramatically increasing**, since more powerful CPU revolution is coming and that will make **the threat of exhaustive attack** on 56-bit DES possible.
- Several other **fatal attacks** on DES has found, such as power analysis attack, differential attack, etc.
- AES should be designed to have the following characteristics:
  - Resistance against all known attacks
  - Speed and code compactness on a wide range of platforms
  - Design simplicity with the key length **128/192/256** bits

Candidate of AES Algorithm

Algorithm	Proposal provider	country
CAST-256	Entrust Inc.	Canada
Crypton	Future System Inc.	Korea
Deal	Richard Outerbridge, Lars Knudsem	Canada
DFC	CNRS-Centre National pour la Recherche Scientifique	France
E2	NTT	Japan
Frog	TecApro International S.A.	Costa Rica
HPC	Rich Schroeppel	USA
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	Australia
Megenta	Deutsche Telekom	Germany
Mars	IBM **	USA
RC6	RSA **	USA
Rijndael	Joan Deamen, Vincent Rijmen **	Belgium
Safer+	Cylink Corp.	USA
Serpent	Ross Anderson, Eli Biham, Lars Knudsen **	UK, Israel, Norway
Twofish	Counterpane **	USA

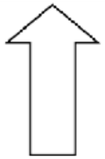
Comparison of AES Candidates

Algorithm	Data (bit)	Key (bit)	Structure	Rounds	Min. Rounds
CAST-256	128	128~256	Ext. Feistel Network	48	40
Crypton	128	~256	Square	12	11
Deal	128	128, 192, 256	Feistel Network	6, 8, 8	10
DFC	128	~256	Feistel Network	8	9
E2	128	128, 192, 256	Feistel Network	12	10
Frog	64~1024	40~1000	Special	8	
HPC	Any	Any	Omni	8	
LOKI97	128	128, 192, 256	Feistel Network	16	38
Megenta	128	128, 192, 256	Feistel Network	6, 8, 8	11
Mars	128	128~1248	Ext. Feistel Network	32	20
RC6	128	~256bytes	Feistel Network	20	21
Rijndael	128, 192, 256	128, 192, 256	Square	10, 12, 16	8
Safer+	128	128, 192, 256	SP Network	8, 12, 16	7
Serpent	128	~256	SP Network	32	17
Twofish	128	128, 192, 256	Feistel Network	16	14

Rounds of Rijndael

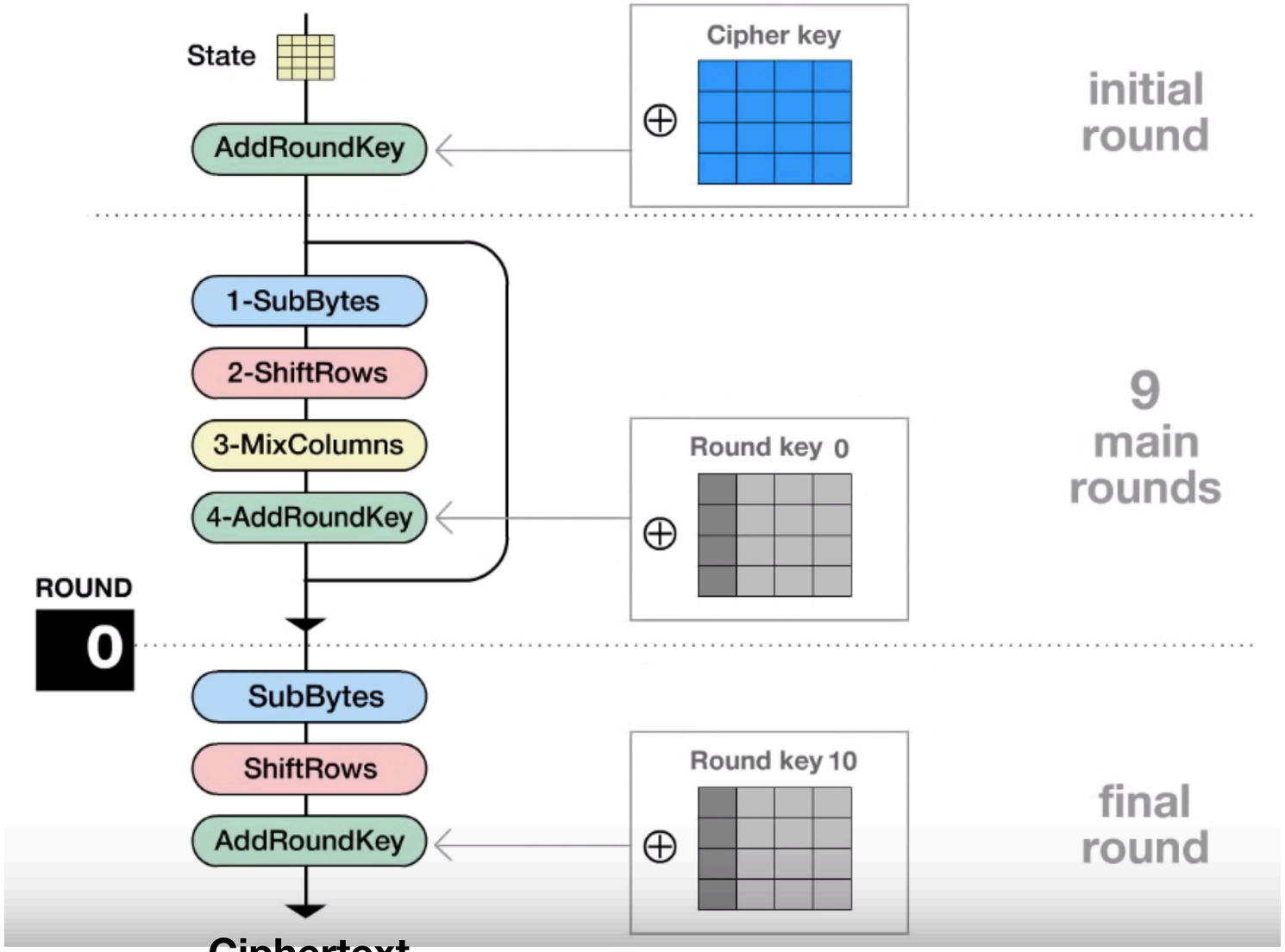
Number of Rounds(Nr)：(Rijndael)

Key block \ Data block	128 bits Nb = 4	192 bits Nb = 6	256 bits Nb = 8
128 bits Nk = 4	Nr = 10	Nr = 12	Nr = 14
192 bits Nk = 6	Nr = 12	Nr = 12	Nr = 14
256 bits Nk = 8	Nr = 14	Nr = 14	Nr = 14



Adopted by FIPS PUB 197

Illustration of AES Encryption Process



Sumber Video: © 2008
Enrique Zabala

http://www.formaestudio.com/rijndaelinspector/

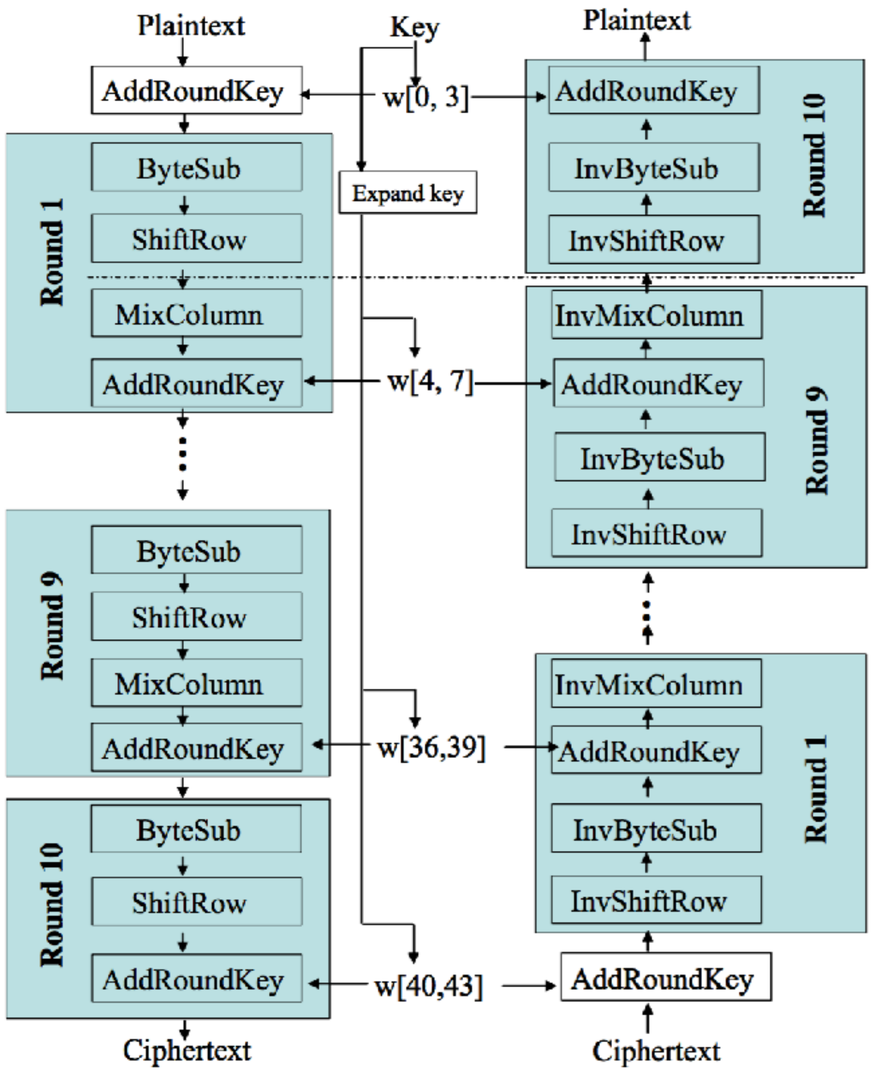
How to navigate through the animation:

> press **Control + F** to get into full screen mode
> use **Enter** key to advance
> use **Slide controller** on bottom to navigate
> press **c** to show/hide the slide controller

Illustration of AES Algorithm

ByteSub is like S-box of DES (diffusion)

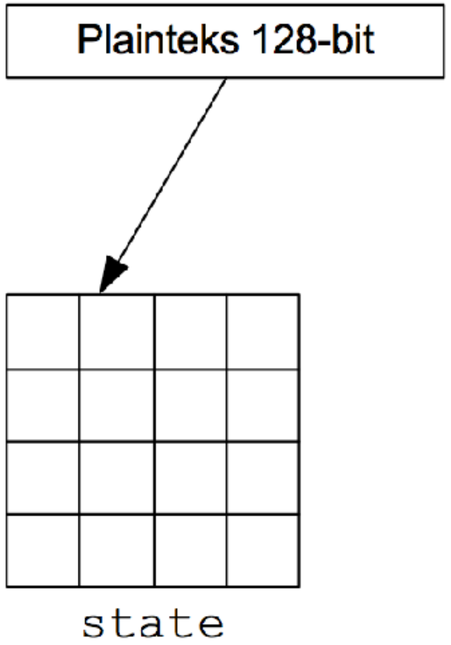
Encryption

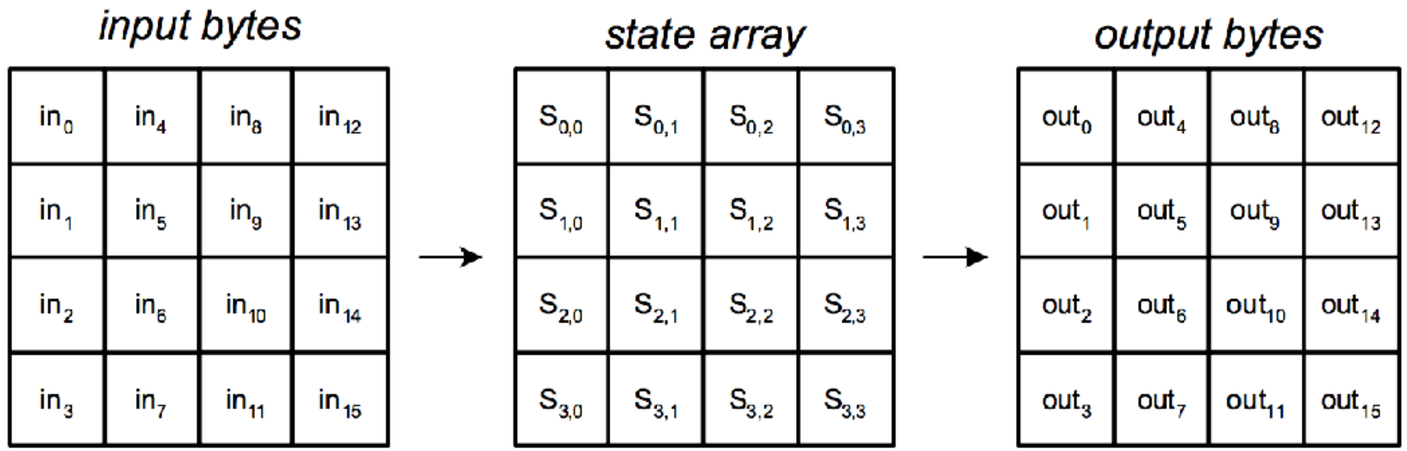


Decryption

State (Data) & CipherKey (Key) of AES

- Plainteks = matrix of byte = **`state`** = $\mathbf{N_{ROWS}}$ **x** $\mathbf{N_{COLS}}$
- Elemen array state diacu sebagai S[r,c], dengan 0 <= r < 4 dan 0 <= c < Nb
- (Nb adalah panjang blok dibagi 32. Pada AES128, Nb = 128/32 = 4).





Operation Elements of AES

- All operations are performed in GF(2^8) with modulo of an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$

  Note that "mod" means "remaining of division"
- **Addition in GF(2^8)** : $A + B$ mod $m(x)$, where A and B are binary representation and "+" means **XOR**
- **Multiplication in GF(2^8)** : $A \cdot B$ mod $m(x)$, and "$\cdot$" means "vector multiplication" (with **AND** gates)
- **Multiplication by *x* in GF(2^8)**: $x \cdot b(x) = b_7x^8 + b_6x^7 + \cdots + b_1x^2 + b_0x$ mod $m(x)$ (with **shift** op)

Bytes Multiplication

- Let $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ and $b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$, where each a_i and b_i is 8-bit representation
- **Polynomials multiplication mod $(x^4 + 1)$:**

$$d(x) = a(x) \otimes b(x) = d_3x^3 + d_2x^2 + d_1x + d_0$$

$$d_0 = a_0 \cdot b_0 \oplus a_3 \cdot b_1 \oplus a_2 \cdot b_2 \oplus a_1 \cdot b_3$$

$$d_1 = a_1 \cdot b_0 \oplus a_0 \cdot b_1 \oplus a_3 \cdot b_2 \oplus a_2 \cdot b_3$$

$$d_2 = a_2 \cdot b_0 \oplus a_1 \cdot b_1 \oplus a_0 \cdot b_2 \oplus a_3 \cdot b_3$$

$$d_3 = a_3 \cdot b_0 \oplus a_2 \cdot b_1 \oplus a_1 \cdot b_2 \oplus a_0 \cdot b_3$$

Example of Addition

$$(57)_{16} + (83)_{16}$$

$$= (01010111)_2 + (10000011)_2$$

$$= (11010100)_2$$

$$= (D4)_{16}$$

Example of Multiplication

$$(57)_{16} \bullet (83)_{16}$$

$$= (01010111)_2 \bullet (10000011)_2$$

$$= (x^6 + x^4 + x^2 + x + 1) \bullet (x^7 + x + 1)$$

$$= (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1)$$

$$\mod \ (x^8 + x^4 + x^3 + x + 1)$$

$$= x^7 + x^6 + 1 = (11000001)_2$$

$$= (C1)_{16}$$

Operations of AddRoundKey

- State_*b* = AddRoundKey(State_*a*, RoundKey)
- State_*b* = State_*a* + RoundKey (XOR operation)
- Note that RoundKey is expanded from the original CipherKey by a KeyExpansion algorithm resulting in a series of **32-bit** words W[*i*]'s
- For 128-bit encryption process, 4 words W[*i*]'s are used as the round key
- For 192-bit encryption process, 6 words W[*i*]'s are used as the round key
- For 256-bit encryption process, 8 words W[*i*]'s are used as the round key

Operation of ByteSub

- State_*b* = ByteSub(State_*a*)
- State_*a* = InvByteSub(State_*b*)
- First find the **inverse of $a_{i,j}$ mod *m*(*x*)** (represented by x_0, x_1, …, x_7), and then use the following **transformation to obtain $b_{i,j}$** (represented by y_0, y_1, …, y_7)

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Table for Quick ByteSub

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

Example: $(d3)_{16}$ → ByteSub → $(66)_{16}$

Operations of ShiftRow

- State_*b* = ShiftRow(State_*a*)
- The 1st row of State_*a* with no shift
- The 2nd row of State_*a* with cyclic left shift C1 bytes
- The 3rd row of State_*a* with cyclic left shift C2 bytes
- The 4th row of State_*a* with cyclic left shift C3 bytes
- State_*a* = InvShiftRow(State_*b*), with cyclic right shift

Nb	C1	C2	C3
4	1	2	3
6	1	2	3
8	1	3	4

Operations of MixColumn

- State_b = MixColumn(State_a) using $c(x)$ = '03'x^3+'01'x^2+'01'x+'02' , i.e., **$b(x) = c(x) \otimes a(x)$**
- State_a = InvMixColumn(State_b) using $d(x)$ = '0B'x^3 + '0D'x^2 + '09'x + '0E', i.e., **$a(x) = d(x) \otimes b(x)$**
- Each block of column (16 bits) is operated under mod x^4+1, and **'01' = $c(x) \otimes d(x)$ (mod x^4+1)**

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02030101 \\ 01020301 \\ 01010203 \\ 03010102 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Contoh

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 26 \\ 7B \\ BD \\ 43 \end{bmatrix} = \begin{bmatrix} 3F \\ 4F \\ F9 \\ 2A \end{bmatrix}$$

$$(02 \bullet 26) \oplus (03 \bullet 7B) \oplus (01 \bullet BD) \oplus (01 \bullet 43) = 3F$$
$$(01 \bullet 26) \oplus (02 \bullet 7B) \oplus (03 \bullet BD) \oplus (01 \bullet 43) = 4F$$
$$(01 \bullet 26) \oplus (01 \bullet 7B) \oplus (02 \bullet BD) \oplus (03 \bullet 43) = F9$$
$$(03 \bullet 26) \oplus (01 \bullet 7B) \oplus (01 \bullet BD) \oplus (02 \bullet 43) = 2A$$

Contoh

$$
\begin{aligned}
(02 \bullet 26) &= (0000\ 0010) \times (0010\ 0110) \\
&= x \times (x^5 + x^2 + x) \ \ \textbf{mod}\ (x^8 + x^4 + x^3 + x + 1) \\
&= (x^6 + x^3 + x^2)\ \textbf{mod}\ (x^8 + x^4 + x^3 + x + 1) \\
&= x^6 + x^3 + x^2 \\
&= (01001100) \\
&= 4C
\end{aligned}
$$

Contoh

$$(03 \bullet 7B) = (0000\ 0011) \times (0111\ 1011)$$
$$= (x + 1) \times (x^6 + x^5 + x^4 + x^3 + x + 1) \textbf{ mod } (x^8 + x^4 + x^3 + x + 1)$$
$$= ((x^7 + x^6 + x^5 + x^4 + x^2 + x) + (x^6 + x^5 + x^4 + x^3 + x + 1)) \textbf{ mod } (x^8 + x^4 + x^3 + x + 1)$$
$$= (x^7 + (1 + 1)x^6 + (1 + 1)x^5 + (1 + 1)x^4 + x^3 + x^2 + (1 + 1)x + 1) \textbf{ mod } (x^8 + x^4 + x^3 + x + 1)$$
$$= (x^7 + x^3 + x^2 + 1) \textbf{ mod } (x^8 + x^4 + x^3 + x + 1)$$
$$= (x^7 + x^3 + x^2 + 1)$$
$$= (1000\ 1101) = 8D$$

$$(01 \bullet BD) = BD = 10111101$$

$$(01 \bullet 43) = 43 = 01000011$$

Contoh

Selanjutnya, XOR-kan semua hasil antara tersebut:

$$
\begin{aligned}
(02 \bullet 26) &= 0100\ 1100 \\
(03 \bullet 7B) &= 1000\ 1101 \\
(01 \bullet BD) &= 1011\ 1101 \\
(01 \bullet 43) &= \underline{0100\ 0011 \oplus} \\
&\quad\ 0011\ 1111 = 3F
\end{aligned}
$$

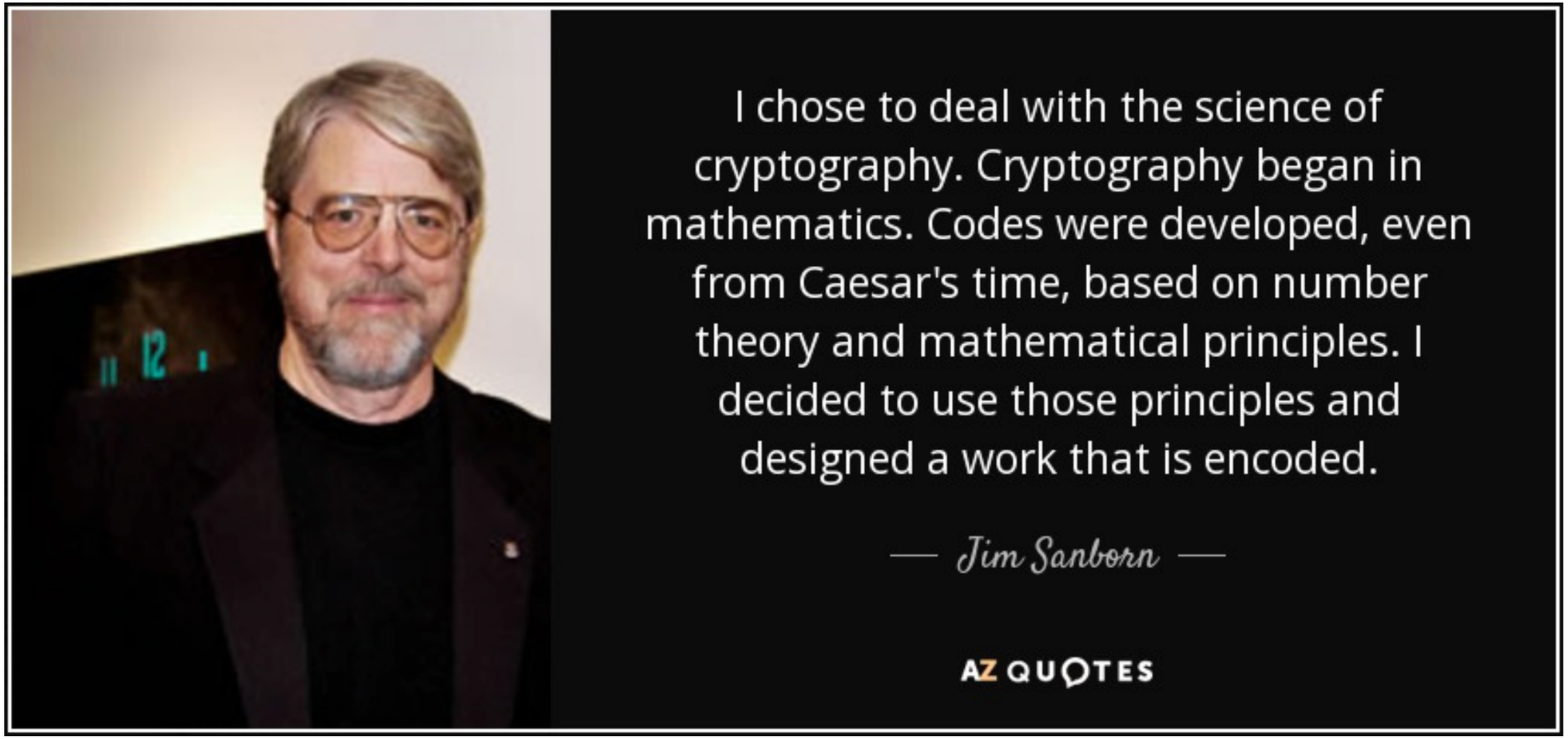
Jadi, $(02 \bullet 26) \oplus (03 \bullet 7B) \oplus (01 \bullet BD) \oplus (01 \bullet 43) = 3F$

Persamaan lainnya diselesaikan dengan cara yang sama.

Merits of the Overall AES Structure

- AES **does not use** a Feistel structure (which used in DES) but process **the entire data block in parallel** during each round using substitution and permutation.
- A round key provided as input is expanded to an array of forty-four **32-bit words** w[i]'s, and **four distinct words (128 bits)** serve the round key for each round.
- The structure is quite simple and four different stages are used: **Substitute bytes**, **Shift rows**, **Mix columns**, and **Add round key.**
- Only use byte-to-byte **substitution**, simple **permutation** (Shift rows), and bit-wise **XOR** operations
- The decryption algorithm is **not identical** to the encryption algorithm

Quote


I chose to deal with the science of cryptography. Cryptography began in mathematics. Codes were developed, even from Caesar's time, based on number theory and mathematical principles. I decided to use those principles and designed a work that is encoded.
— Jim Sanborn —
AZ QUOTES

THANK YOU!