# ISC
# MidSem Discussion and Solution
# B Tech III CSE
# (**March 2023**)

Dhiren Patel

# Q1 A1 (03 marks)

- Use a phrase “Smith captioned Aussy much better than Cummins to defeat India” to define a key of 5x5 Playfair cipher.
- Encrypt “India at WTC” →
- IN DI AX AT WT CX
- HP UM OV OM XI/J OQ
- If Z is used – cipher text
- HP UM NV OM XI/J NQ
- Some used W too… and X and Z both too

| S | M | I/J | T | H |
|---|---|---|---|---|
| C | A | P | O | N |
| E | D | U | Y | B |
| R | F | G | K | L |
| Q | V | W | X | Z |

# Q1 A2 (2 marks)

- Encrypt the text “meet me at ten pm near gate” using Rail Fence Cipher (of depth 2) and Caesar cipher with key 2.
- Rail Fence cipher
- m e m a t n m e r a e
- e t e t e p n a g t x
- Caesar cipher
- oggv og cv vgp ro pgct icvg

# Q1 B (3 marks) – 1.5 marks each

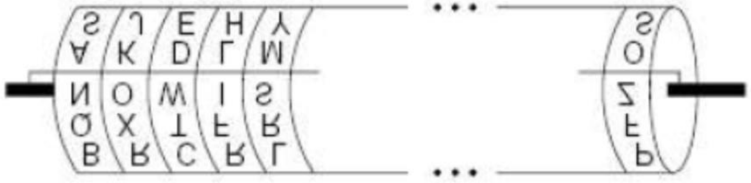
- **Discuss security of One-time-pad. What is two-time pad?**
- A random key sequence “added” to a nonrandom plaintext message produces a completely random cipher-text message and no amount of computing power can break that
- Key – completely Random, used only once (from synchronized key pad), long running key, Encryption is XOR (or n Caesar ciphers), Output – completely random, most secure cipher
- Practical Implementation is difficult!!
- Two time pad – key is used twice. Vulnerable.

# How ChatGPT can threaten information security?

- ChatGPT maker OpenAI and its investor Microsoft “are able to read queries” typed into AI-powered chatbots. (The query will be visible to the organisation providing the [chatbot]) - could reveal sensitive information through their search queries
- Threat actors are exploiting the popularity of OpenAI's ChatGPT chatbot to distribute malware for Windows and Android, or direct unsuspecting vitims to phishing pages
- ChatGPT can aid in malware development. For example, a user with a rudimentary knowledge of malicious software could use the technology to write functional malware.
- Malware authors can also develop advanced software with ChatGPT, like a **polymorphic virus**, which changes its code to evade detection.

# Discuss Jefferson cylinder.

- The *Jefferson cylinder* is a simple (mechanical) cipher, implements a poly-alphabetic substitution cipher while avoiding complex machinery, extensive computations, and Vigenère table.
- A solid cylinder 6 inches long is sliced into 36 disks. The periphery of each disk is divided into 26 parts – with letters in different ordering.
- Each of the 36 wheels is individually rotated to bring the appropriate character (matching the plaintext block) into position along the reference line. One out of other 25 parallels is selected as the ciphertext to transmit.
- The ciphertext is decrypted by rotating each of the 36 disks to obtain characters along a fixed reference line matching the ciphertext.
- The other 25 reference positions are examined for a recognizable plaintext.
- Reordering disks (1 through 36) alters the polyalphabetic substitution key (36! orderings)



# Q2 (Any three) 2 marks each

1. What are the Side Channel Attacks? Discuss Timing attack and its countermeasures.
2. How Cryptographic hash function can be used for message authentication and in software licensing?
3. List classical and modern Steganography techniques.
4. List properties of cryptographic hash function (CHF). How CHF can be constructed from a symmetric key block cipher?
5. List critical infrastructures. What was Stuxnet?

# What are the Side Channel Attacks? Discuss Timing attack and its countermeasures

- Indirect attacks, based on extra information that can be gathered based on how protocol or algorithm is implemented (rather than flaws found in a cryptanalysis) -
- Information emitted (leaked) through a side channel - Timing information, power consumption, electromagnetic leaks, and sound are examples
- Timing attack - based on measuring how much time various computations take to perform (watches data movement into and out of the CPU or memory on the hardware)
- a random delay can be added to deter timing attacks
- (attack - computation times are quantized into discrete clock cycle counts) - countermeasure is to design the software to be isochronous, that is to run in an exactly constant amount of time, independently of secret values

# How Cryptographic hash function can be used for message authentication and in software licensing?

- Plain text, Shared Secret, Hash (MAC)
- License key are generated using Hash of Software distribution package (executable / source files) + Machine identity (MAC address of NIC or CPU ID or OS license key etc.)
- Installation time – customized License keys (and hash of software image) are stored at secure location on computer/network
- While execution of software – hash is computed and matched with license keys/hash

# List classical and modern Steganography techniques

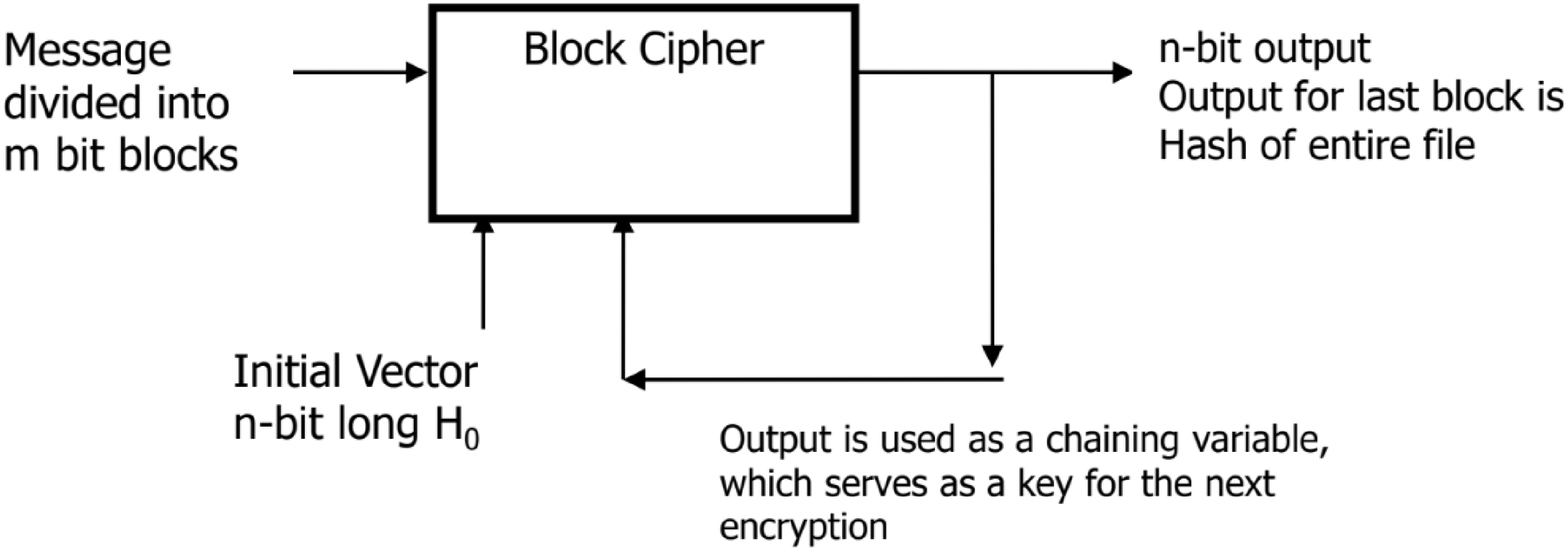
- Steganography's goal is to prevent the detection of a secret message.
- Classical techniques –
- Prisoners used a "tap code" to communicate,
- hidden msg - letters in words of a document - e.g. collect second letter from each word,
- Pin puncture,
- Over written characters,
- writing using invisible ink,
- Modified alphabet
- IR controls
- Colored glasses to filter wavelengths

# Modern techniques

- The secret information is inserted or "hidden" into the “container data” <any type of digital data file>,
- Bits in Images - Low-Bit Encoding (image)
- Spread Spectrum
- Echo Data Hiding (audio)
- Perceptual Masking (audio–differential sounds)
- Discrete Cosine Transform (video)
- Textual steganography (spacing, coding)
- unused space in the packet headers
- Blank areas on Memory, HTML code,
- Holography, Pagers

# List properties of CHF. How CHF can be constructed from a symmetric key block cipher?

- Properties:
- Operational: H() should work on any input length and should produce output of fixed size
- Deterministic: the same message always results in the same hash
- One-Way Function: You cannot reverse the cryptographic hash function to get to the data.
- Quick: It is quick to compute the hash value for any given message.
- Collision Resistance: It is infeasible to find two different messages that produce the same hash value.
- Avalanche Effect: every minor change in the message results in a major change in the hash value.
- Non Predictable: The hash value shouldn’t be predictable from the given string and vice versa.



Message divided into m bit blocks

Block Cipher

n-bit output
Output for last block is
Hash of entire file

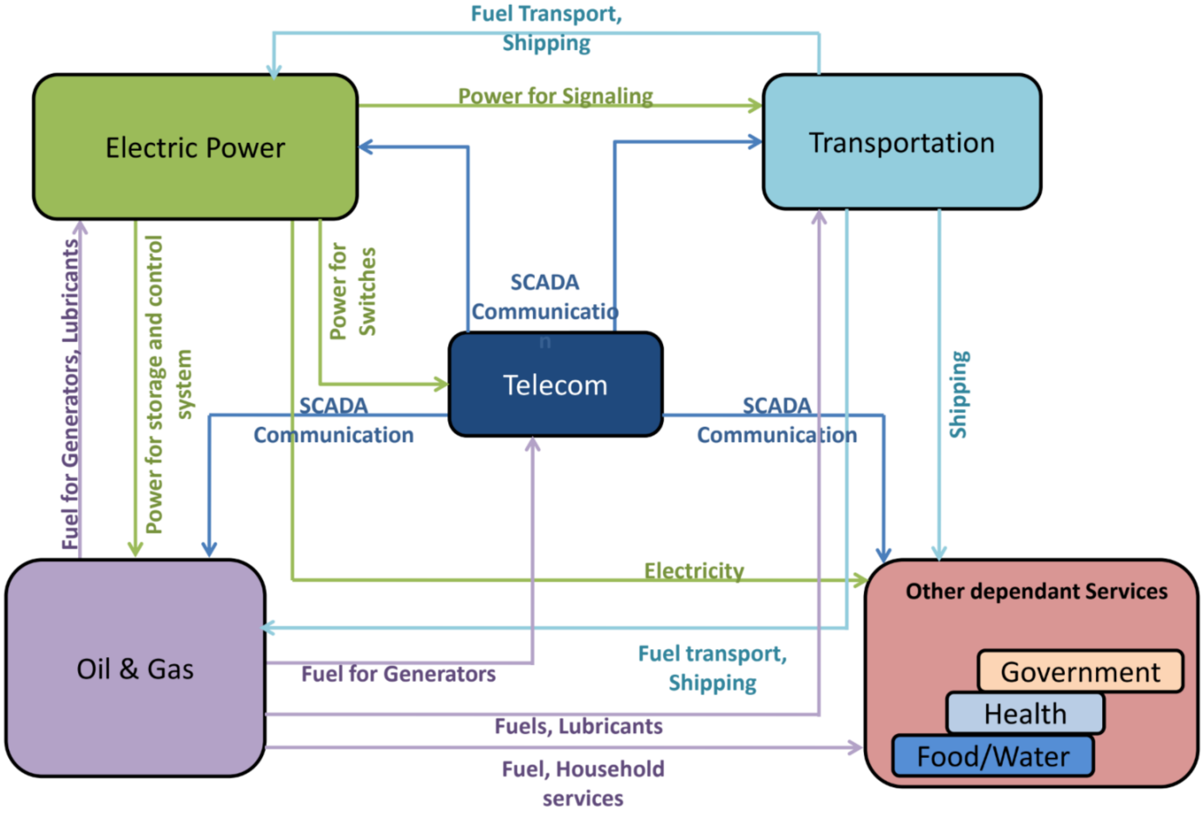
Initial Vector
n-bit long $H_0$

Output is used as a chaining variable, which serves as a key for the next encryption

Hash Function Using A Block Cipher

# List critical infrastructures. What was Stuxnet?

- Electric power, Transportation, Telecom, Oil and gas, Govt services, (Health, Food, water)



# Stuxnet

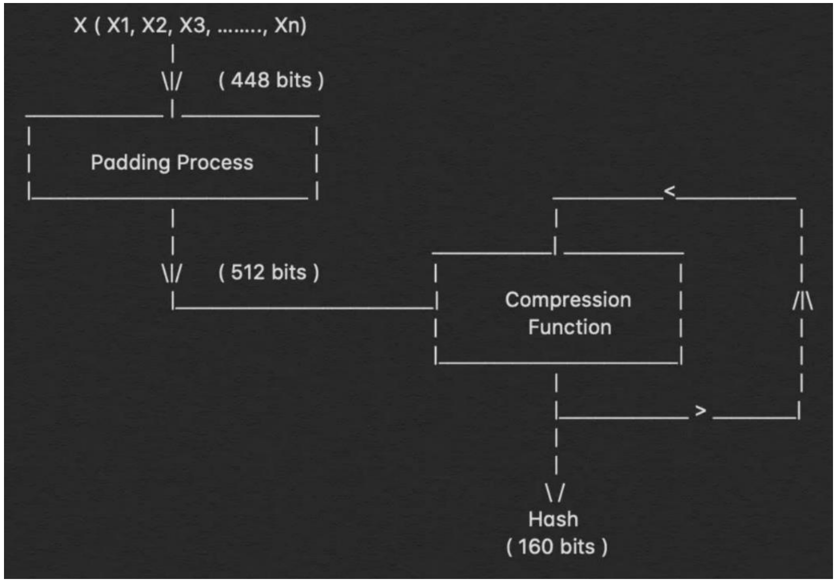
- Stuxnet - a malicious computer worm first uncovered in 2010.
- It was tailored as a platform for attacking modern SCADA and PLC systems.
- Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart
- Stuxnet is believed to be responsible for causing substantial damage to the nuclear program of Iran.

# Q2 B Answer any one (4 marks)

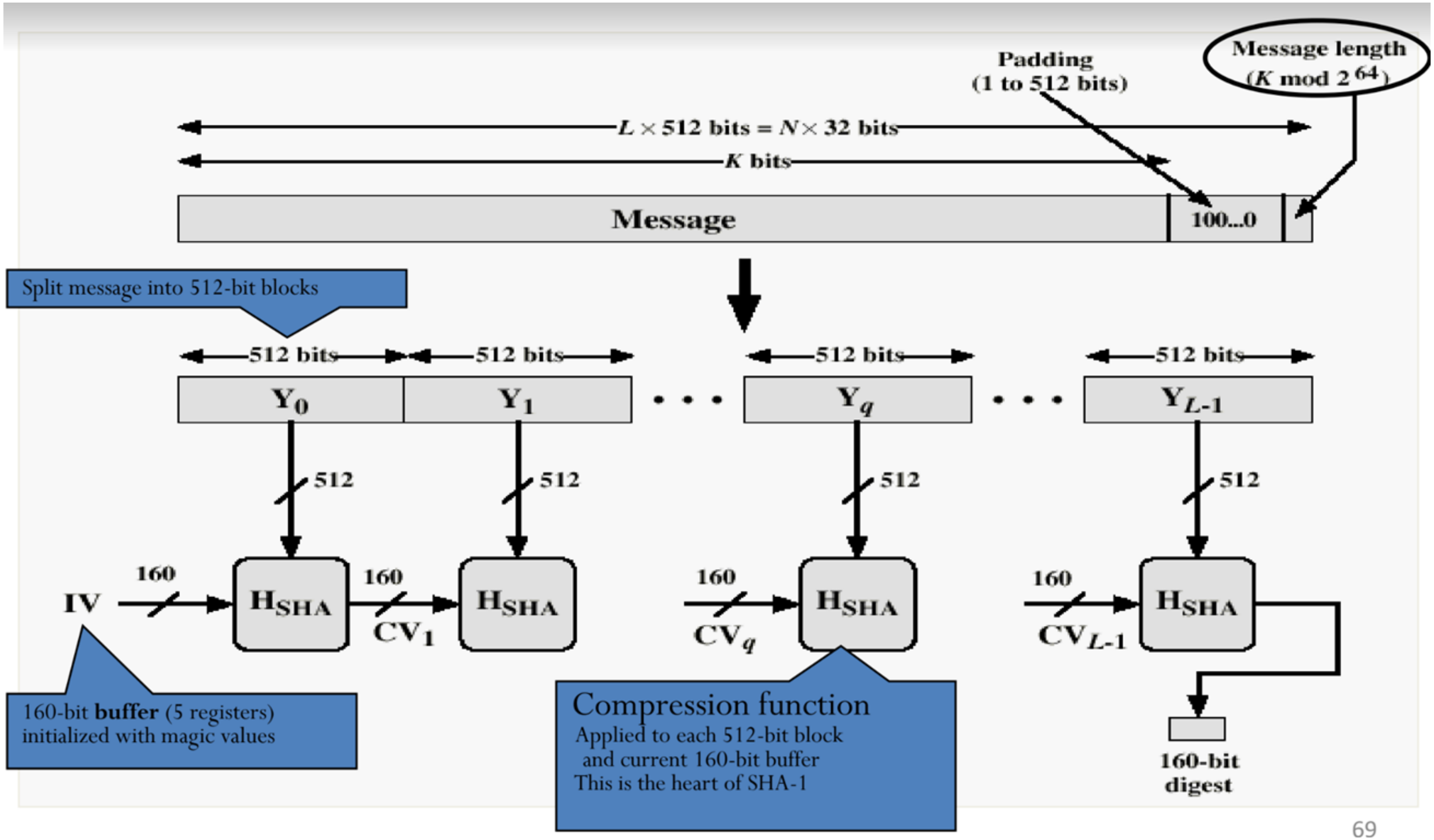
1. Discuss AES and its design
2. Discuss SHA1 and its design

# SHA-1

- Secure Hashing Algorithm, 160 bit cryptographic hash function, NIST FIPS – 180
- Padding (448 bits (1 followed by 0s) + 64 bit message length)
- Message blocks are processed with Initial value of 5 words of 32 bits each – A,B,C,D,E; transformed to 160 bits of hash.
- A = 0x67452301
- B = 0xEFCDAB89
- C = 0x98BADCFE
- D = 0x10325476
- E = 0xC3D2E1F0



# SHA-1



Split message into 512-bit blocks

160-bit **buffer** (5 registers)
initialized with magic values

Compression function

Applied to each 512-bit block
and current 160-bit buffer
This is the heart of SHA-1

# SHA 1 Functions

- Each function ft takes three words B, C and D as input, and produces one word as output, Ks are constants
- First 20 Rounds
- f(1) = (B and C) or ((not B) and D) , k(1) = 0x5A827999

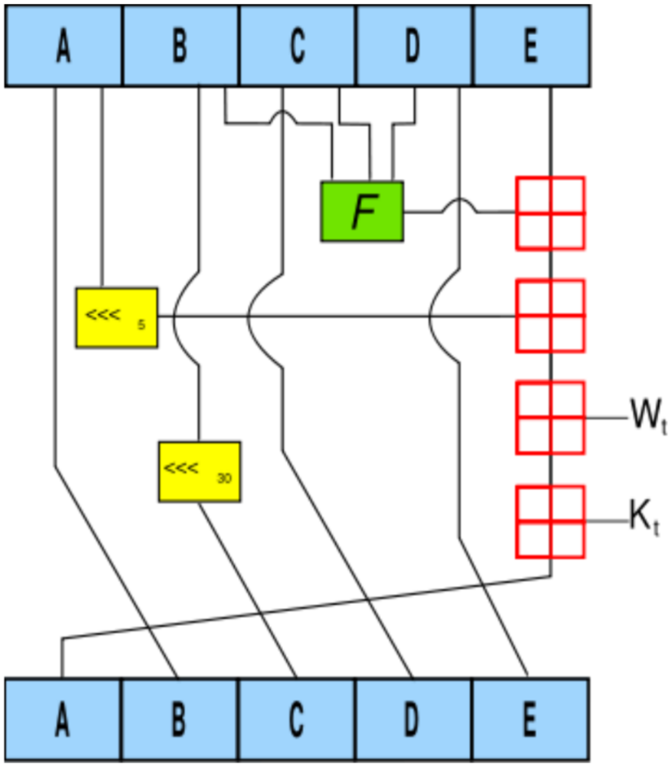
- Next 20 Rounds
- f(2) = B xor C xor D , k(2) = 0x6ED9EBA1

- Next 20 Rounds
- f(3) = (B and C) or (B and D) or (C and D),k(3) = 0x8F1BBCDC

- Next 20 Rounds
- f(4) = B xor C xor D, k(4) = 0xCA62C1D6

# SHA-1 one operation

- For t=0 to 79
- TEMP = (a <<< 5) + ft
- (b,c,d) + e + Wt + Kt
- e = d
- d=c
- c=b <<< 30
- b = a
- a = TEMP



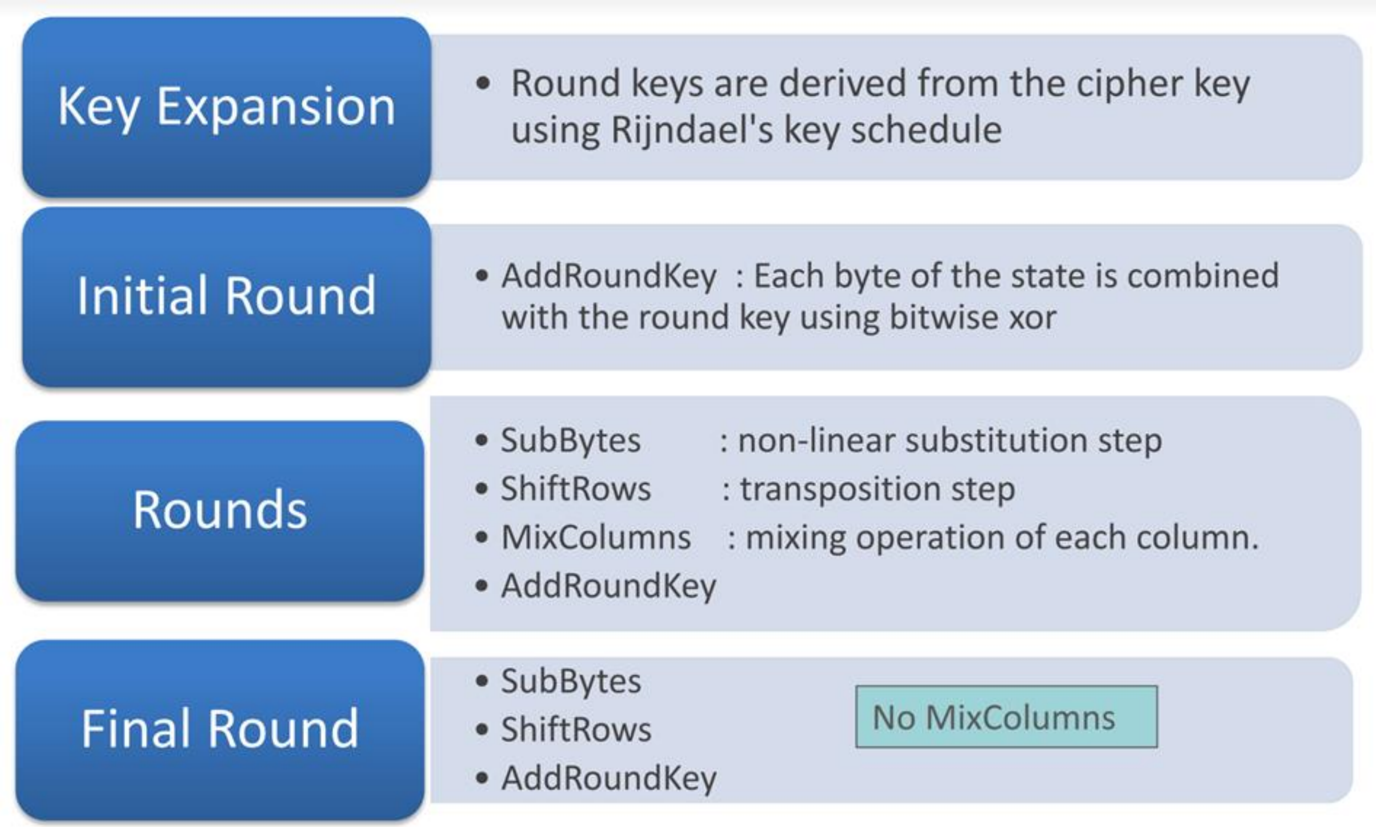
# AES

- AES stands for Advanced Encryption Standard, (Declared as standard) in 2001 – NIST FIPS 197
- AES is 128 bit Symmetric Block Cipher (msg. block size is 128 bit)
- Number of rounds in AES depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)
- The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition
- (invented as Rijndael cipher by Vincent Rijmen and Joan Daemen - KUL)
- an iterative rather than feistel cipher treats data in 4 groups of 4 bytes, operates an entire block in every round

# AES

- it uses GF($2^8$) with irreducible polynomial

$$x^8 + x^4 + x^3 + x + 1$$



Key Expansion

- Round keys are derived from the cipher key using Rijndael's key schedule

Initial Round

- AddRoundKey : Each byte of the state is combined with the round key using bitwise xor

Rounds

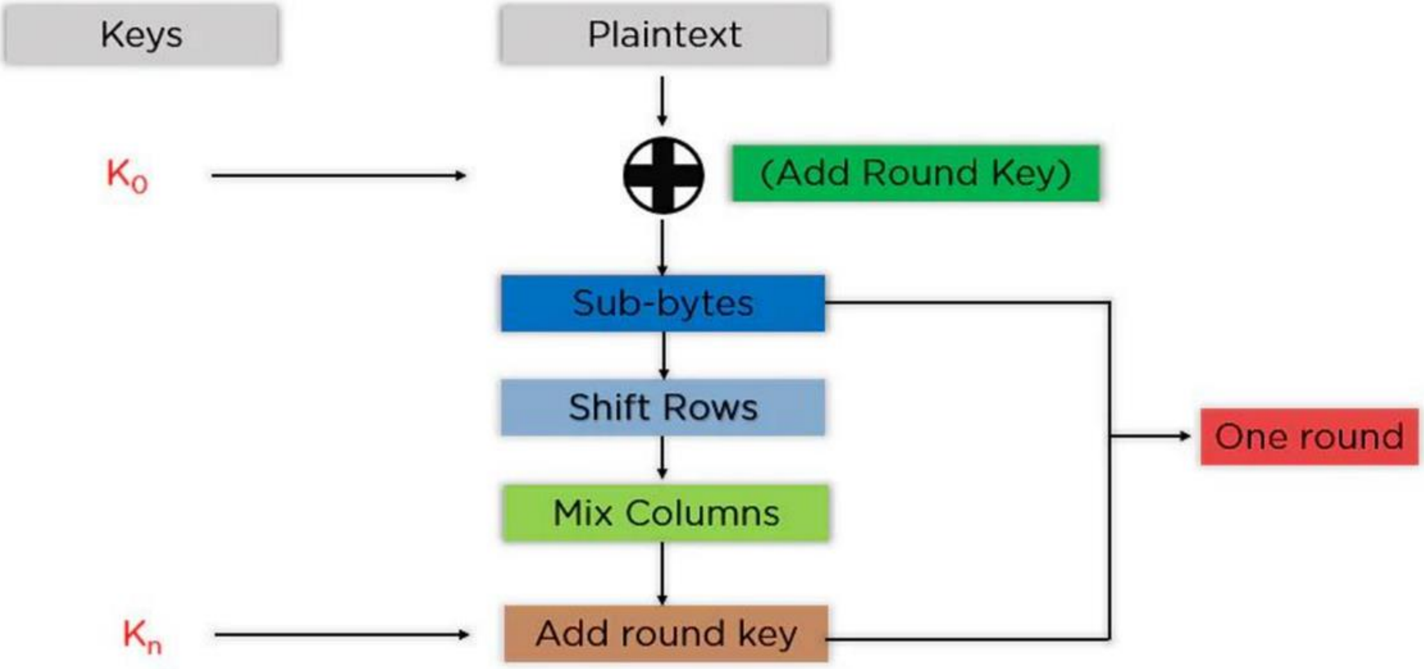
- SubBytes : non-linear substitution step
- ShiftRows : transposition step
- MixColumns : mixing operation of each column.
- AddRoundKey

Final Round

- SubBytes
- ShiftRows
- AddRoundKey

No MixColumns

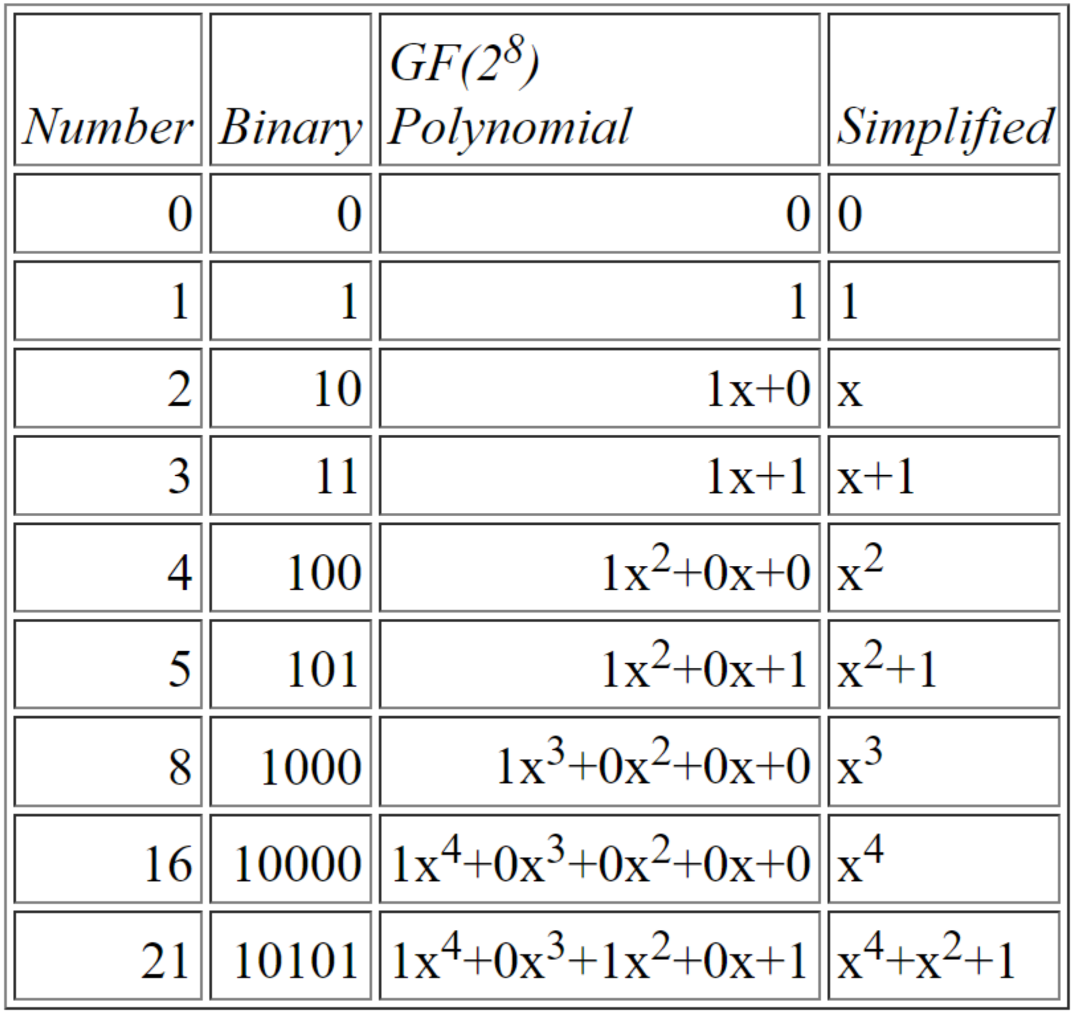
# AES one round



# Field (Additional Material)

- A field can be defined as a set of numbers that we can add, subtract, multiply and divide together and only ever end up with a result that exists in our set of numbers.
- Finite Field: A field with finite number of elements, also known as Galois Field
- (Named after a mathematician Evariste Galois who died at age of 20 (1811-1832) - post Napoleon France – solved a problem that had been open for 350 years).
- His theory uncovers a relationship between the structure of groups and the structure of fields. It then uses this relationship **to describe how the roots of a polynomial relate to one another**
- E.g. GF(2) = mod 2 arithmetic and GF(8) = mod 8 arithmetic.

# Members of a field of size $p^n$ are equivalent to polynomials of degree up to $n$, with coefficients chosen from integers modulo$p$



| *Number* | *Binary* | *GF($2^8$) Polynomial* | *Simplified* |
|---:|---:|---:|:---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 2 | 10 | $1x+0$ | $x$ |
| 3 | 11 | $1x+1$ | $x+1$ |
| 4 | 100 | $1x^2+0x+0$ | $x^2$ |
| 5 | 101 | $1x^2+0x+1$ | $x^2+1$ |
| 8 | 1000 | $1x^3+0x^2+0x+0$ | $x^3$ |
| 16 | 10000 | $1x^4+0x^3+0x^2+0x+0$ | $x^4$ |
| 21 | 10101 | $1x^4+0x^3+1x^2+0x+1$ | $x^4+x^2+1$ |

# Use of Galois Field in AES

- The big advantages of working in a finite field are:
- Numbers stay small--everything in GF($2^8$) is always one byte, even after multiplication or division.
- Inverses exist for each operation, which makes decryption possible.
- The number of elements is always a power of a prime number, denoted as GF($p^n$).
- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p.
- Addition, subtraction, multiplication, and division can be done without leaving the field GF(p).

# GF in AES

- AES uses arithmetic in the finite field GF($2^8$ ) with irreducible (prime) polynomial.
- $m(x) = x^8 + x^4 + x^3 + x + 1$ which is (1 0001 1011) in binary or {11B} in Hex-decimal
- Irreducible polynomial is a polynomial that is not a product of two other polynomials.