MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Intro to Crypto

Greg Boyd

gregboyd@mainframecrypto.com

August 2019

Copyrights and Trademarks

- Copyright © 2019 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 30+ years

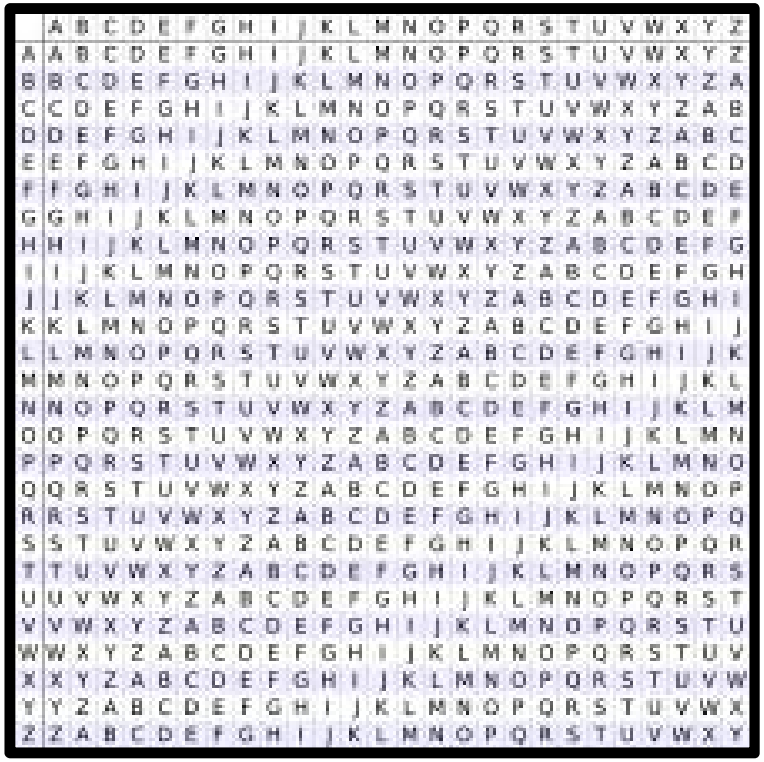
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

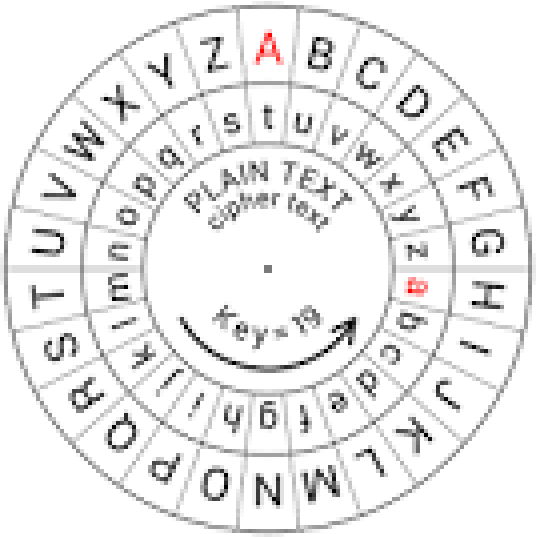
Agenda – Intro To Crypto

- Some background
- Crypto Functions
  - Symmetric algorithms
  - Asymmetric algorithms
  - Hashes
  - PIN Support

Historical Ciphers

Scytale





Caesar Cipher, Key = 7

MAINFRAME

THPUMYHTI

Vigenere Square, Key = BOYD

MAINFRAME

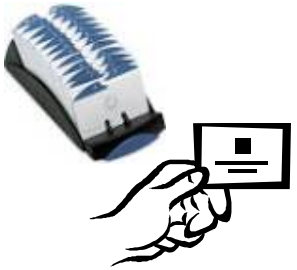
BOYDBOYDB

NOGQGFYPF

Today's Business Environment

Hospital

Government



Remote User

Trust
Confidentiality
- Trade Secrets
- Business transactions

Privacy
- Personal Information

Accountability/ Auditability

Internet/ Intranet

Transportation Distribution

Insurance

Finance

Endless Possibilities, but they require confidence

What is Cryptography?

Cryptography (or cryptology; from Greek κρυπτός, *kryptos*, "hidden, secret"; and γράφω, *gráphō*, "I write", or -λογία, *-logia*, respectively)[1] is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

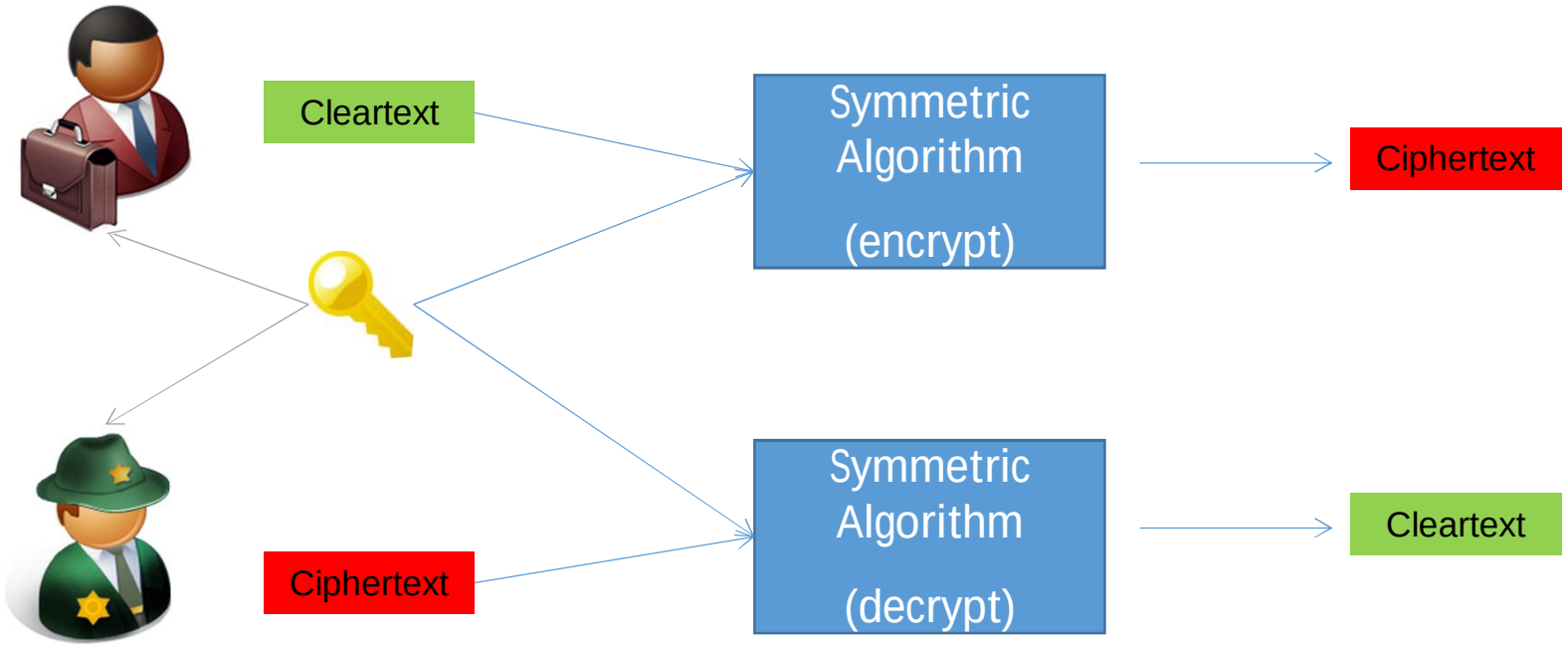
From Wikipedia

Cryptographic Functions

- Data Confidentiality
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA, Diffie-Hellman, ECC
- Data Integrity
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- Financial Functions
- Key Security & Integrity

Confidentiality – Symmetric Algorithms

- Symmetric - One key shared by both parties

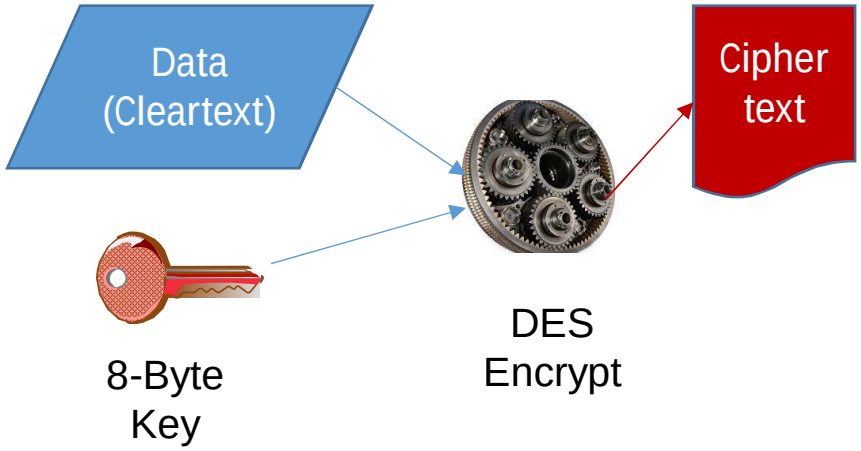


Symmetric Algorithms

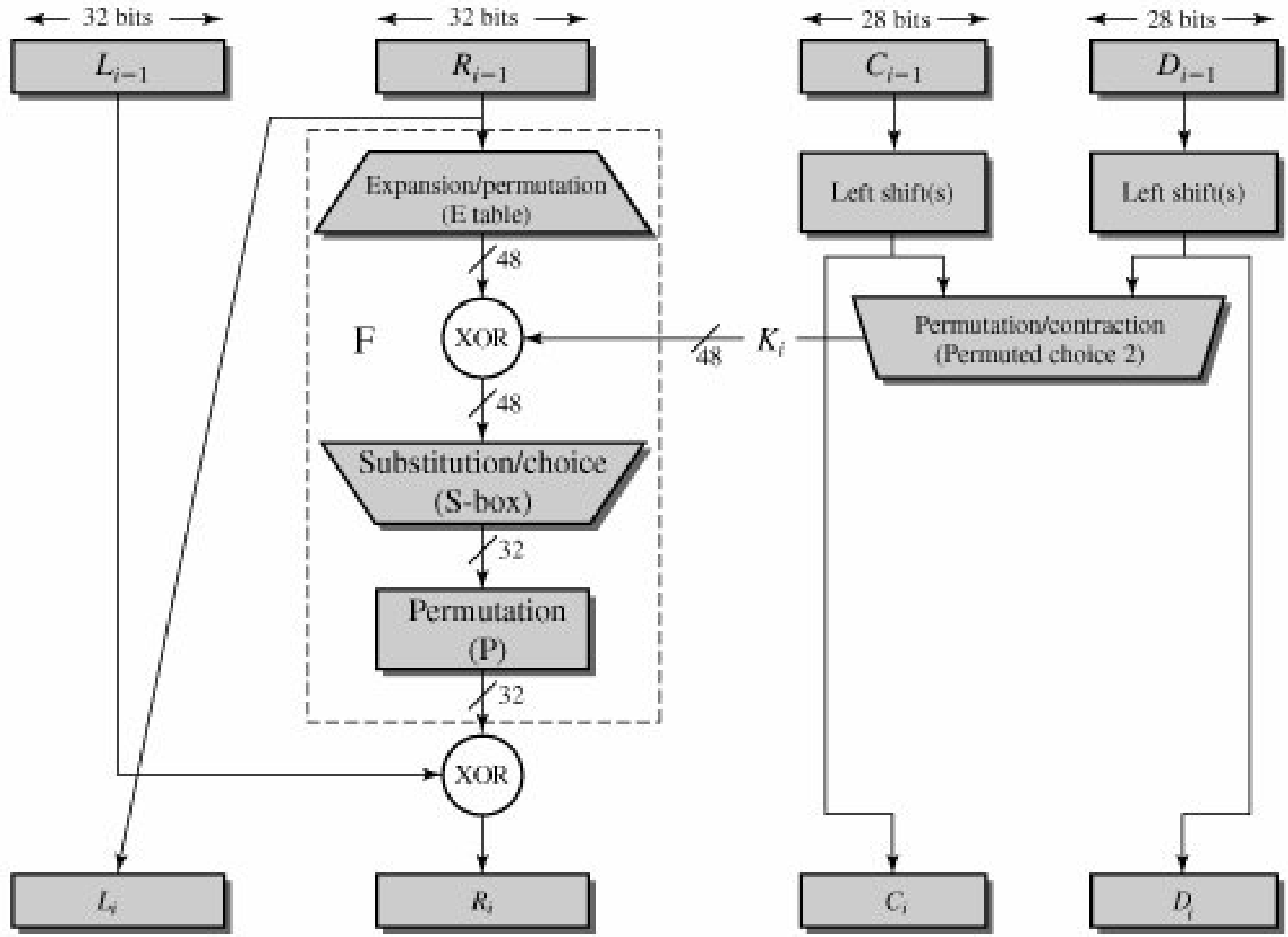
- Symmetric
  - DES/TDES*
  - AES*
  - Blowfish / Twofish
  - Serpent
  - IDEA
  - RC2 / RC4
  - Skipjack
  - ....

*Supported on IBM Hardware

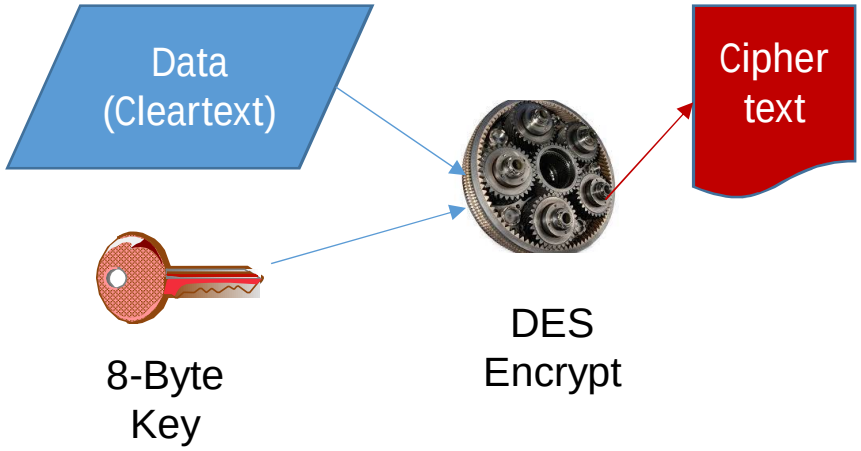
DES Algorithm - Encrypt

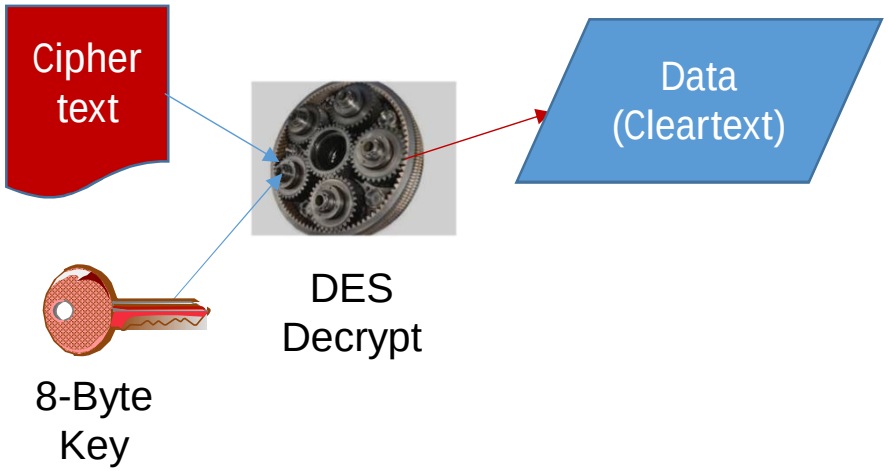


Single Round of DES Encrypt

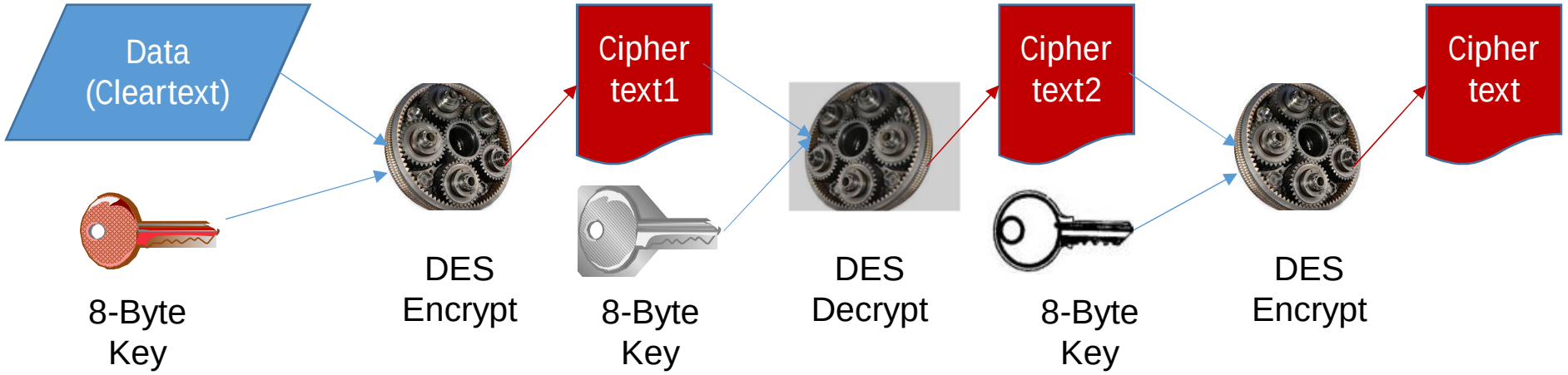


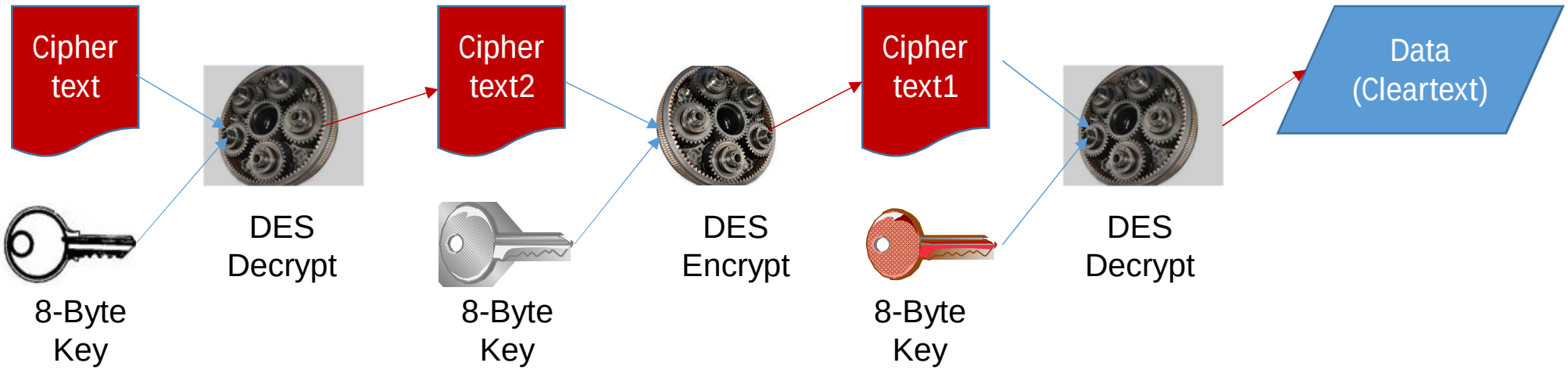
DES Algorithm - Decrypt



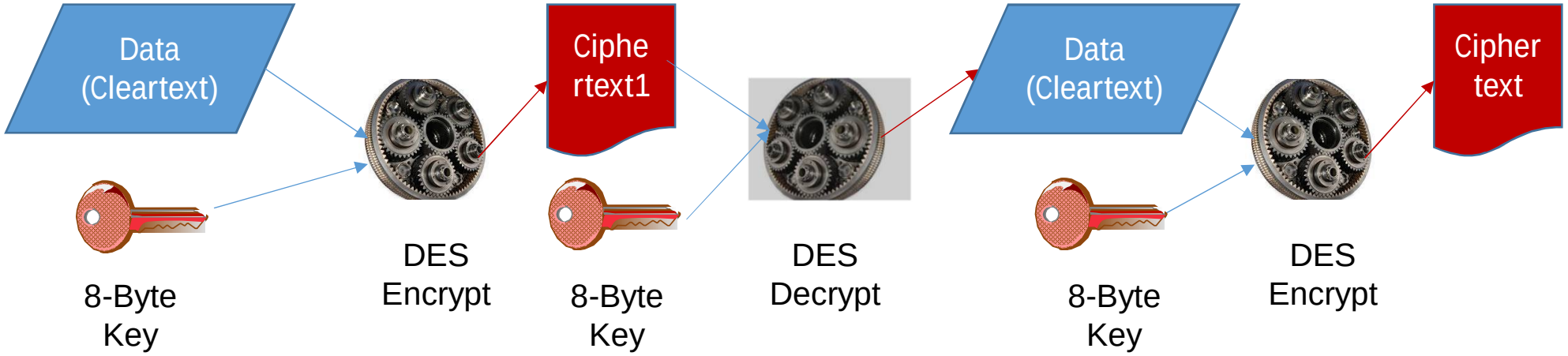


TDES Algorithm





TDES Algorithm

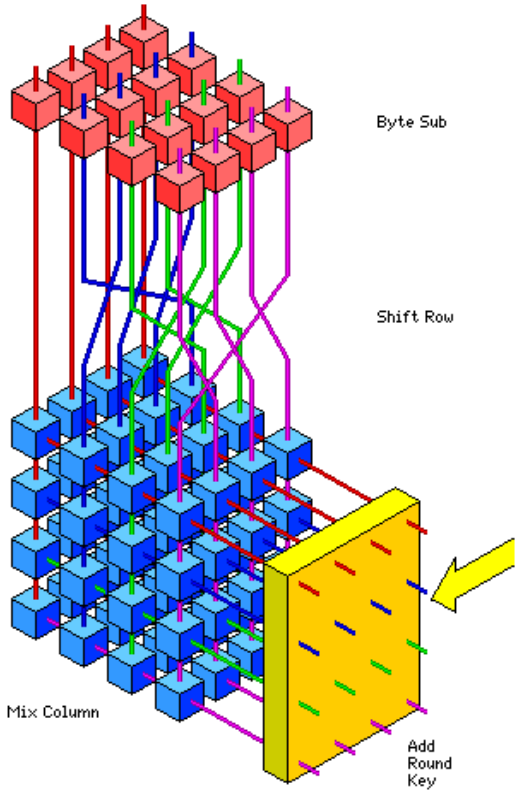


TDES – Disallowed/Deprecated

- Transition the Use of Cryptographic Algorithms and Key Lengths (NIST SP 800-131A Rev. 2)
  - Two-key TDEA Encryption – Disallowed
  - Two-key TDEA Decryption – Legacy Use
  - Three-key TDEA Encryption – Deprecated thru 2023, Disallowed after 2023
  - Three-key TDEA Decryption – Legacy Use

https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

Data Confidentiality - AES

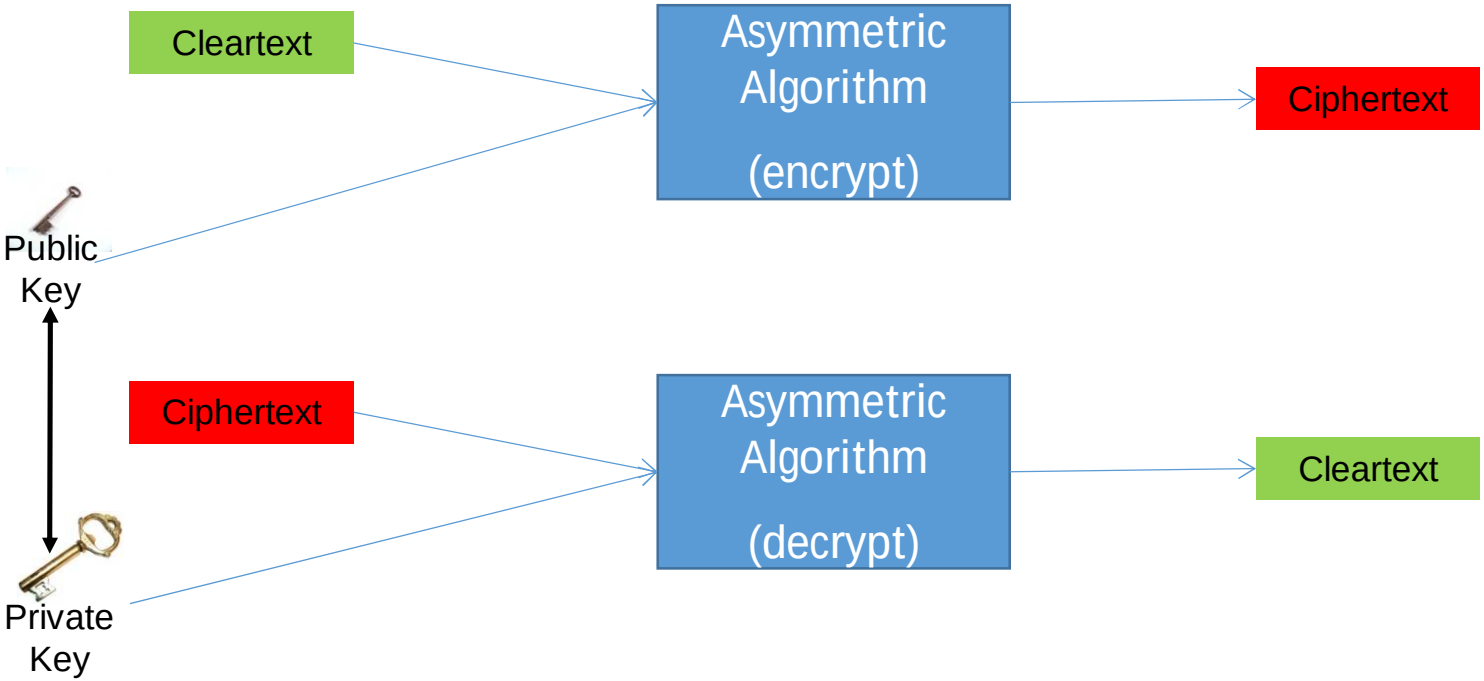


- Rijndael Algorithm
  - Block Cipher (16-byte blocks)
  - 128-, 192-, 256-bit key length
    - 128 bit key=> 3.4x10**38 (340 Undecillion)
    - 192 bit key=> 6.2x10**57 (6.2 Octodecillion)
    - 256 bit key=> 1.1x10**77 (almost a Googol)
  - Multiple round
  - Four steps per round (Byte substitution, shift row, mix column, add round key)

Image from http://www.esat.kuleuven.ac.be/~rijmen/rijndael

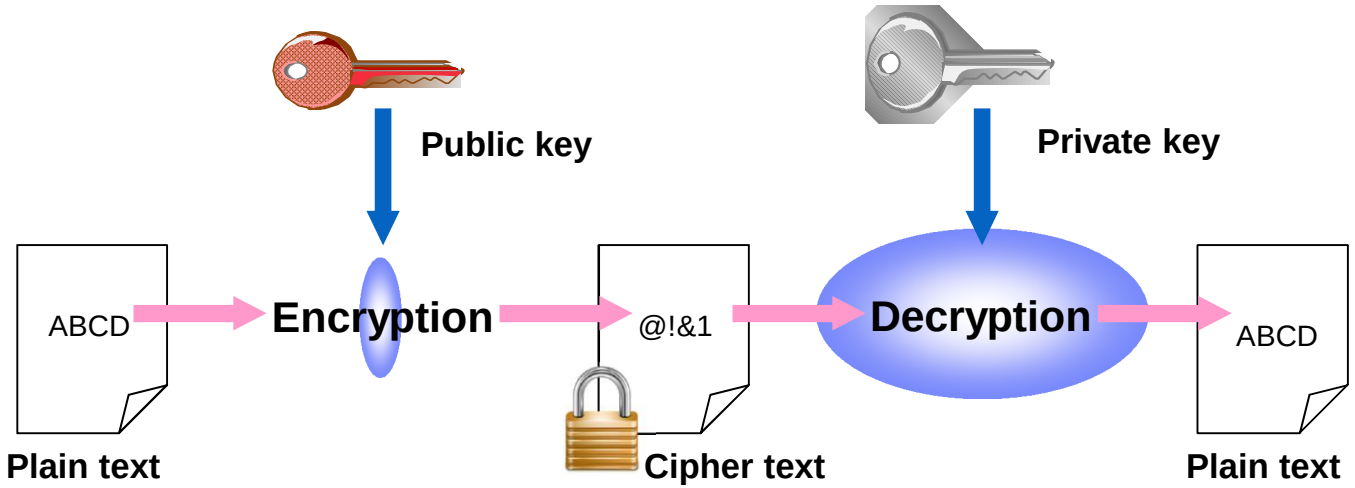
Secrecy Algorithms - Asymmetric

- Asymmetric – two different, but mathematically related keys (public and private)



Asymmetric Algorithms

- Public Key Architecture - PKA
  - RSA - factorization
  - Diffie-Hellman - logarithmic
  - Elliptic Curve – point multiplication



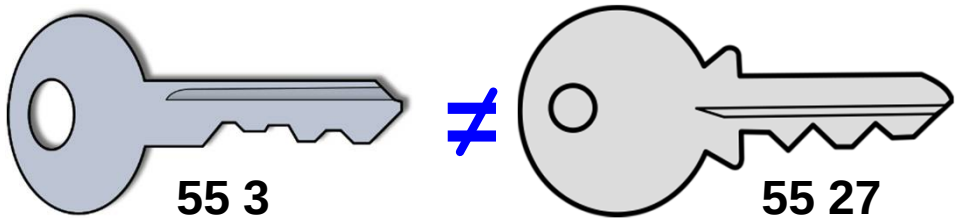
Generating RSA Keys

- RSA Keys consists of two parts, a modulus (N) and an exponent (E for the public key; D for the private key)
  - Public Key => N E
  - Private Key => N D
- The modulus is calculated by multiplying two prime numbers (P & Q) together
  - P = 5 Q = 11 (prime numbers and should be very large)
  - N = P x Q => 5 x 11 = 55
- Next, select an odd number, E, that will be the exponent for the public key
  - Good values include 3 or 65537 (64K+1) or 5, 17 or 257 with HCR77C0

    Public Key=> N E => **55 3**
- Finally, calculate the exponent for the private key, D, where

  1 = (D * E) MOD ((P-1)(Q-1)) **=> 1 = (D * 3) MOD ((5-1)(11-1))**
  - In our example, solve for 1 = (D * 3) MOD 40 => D = 27!

    Private Key => N D => **55 27**



Encipher the Message ‘MFC’

Public Key (N E) => 55 3

Private Key (N D) => 55 27

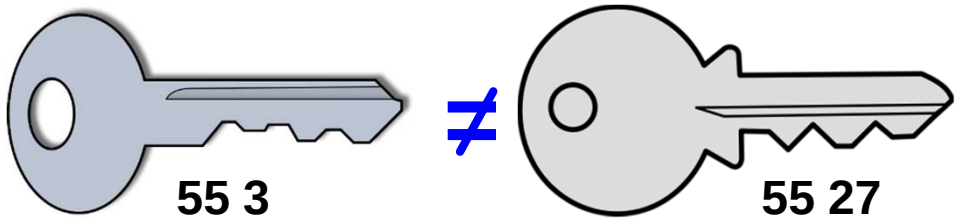
Convert characters to numeric (a=1, b=2, c=3, etc.)

‘M’ = 13; ‘F’ = 6; ‘C’ = 3;

ciphertext = (cleartextE) Mod N**

- For ‘M’ (13**3) MOD 55 => 2197 MOD 55 = 52
- For ‘F’ (6**3) MOD 55 => 216 MOD 55 = 51
- For ‘C’ (3**3) MOD 55 => 9 MOD 55 = 27

Ciphertext is 52 51 27



Decipher the message 52 51 27

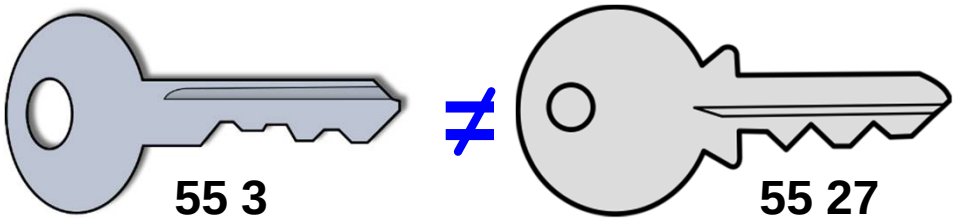
Public Key (N E) => 55 3

Private Key (N D) => 55 27

Cleartext = (ciphertextD) MOD N**

- For 52 52**27 MOD 55 = 13
  (52**27 = 2.148276996714467901343670681657 2e+46)
- For 51 51**27 MOD 55 = 6
  (51**27 = 1.271729526401389390382398199869 9e+46)
- For 27 27**27 mod 55 = 3
  (27**27 = 4.434264882430377699482496306191 5e+38)

- My decrypted message is 13 6 3 => “M” “F” “C”



ECC Algorithm

Effective Key Size (bits)		
Symmetric	RSA	ECC
80	1024	163
112	2048	224
128	3072	256
192	7680	384
256	15360	512
From NIST SP 800-57 Part 1 (Table 2) at www.nist.gov		

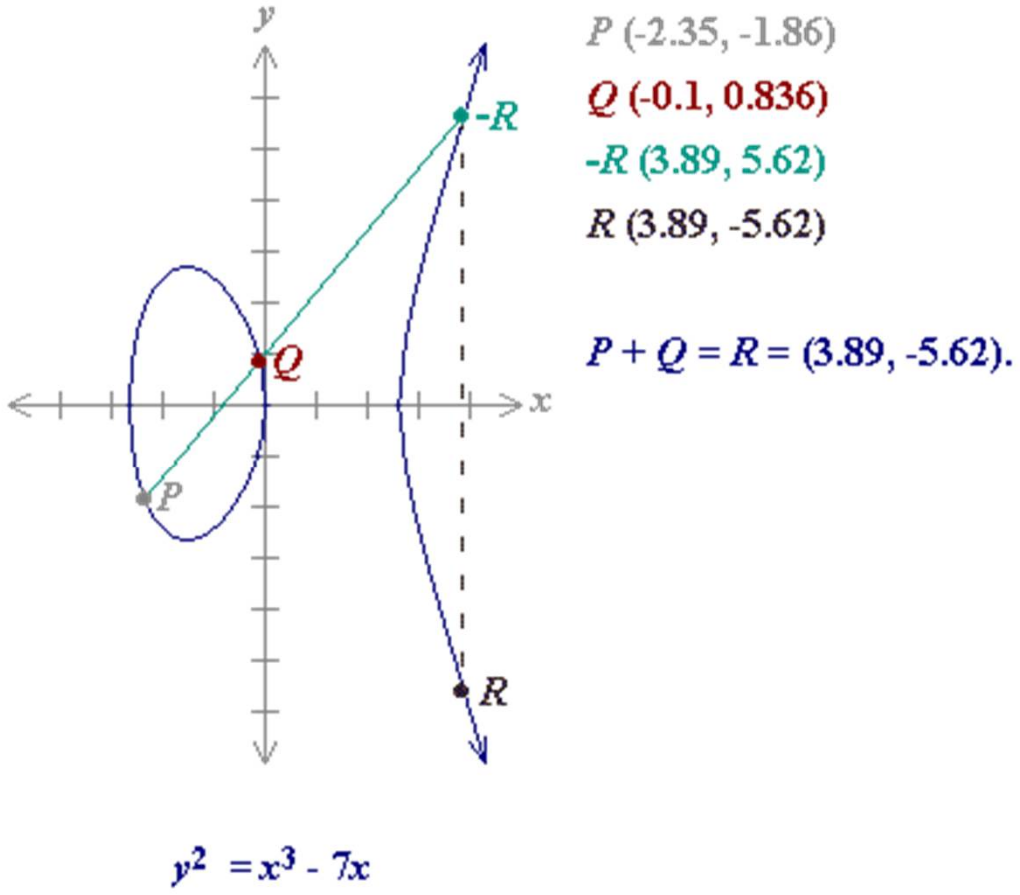
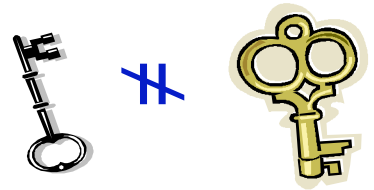
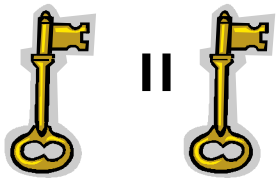


Image from crypto.stackexchange.com

Why Asymmetric and Symmetric Keys?

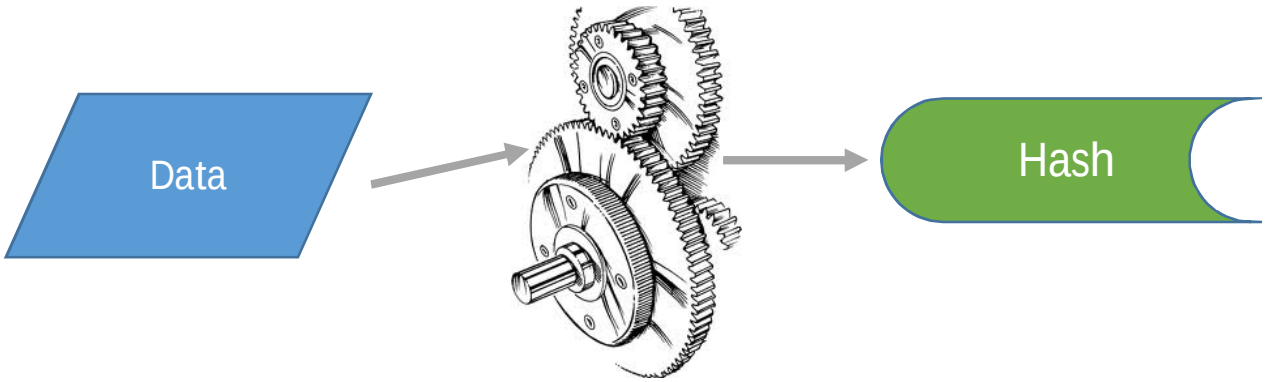


- Asymmetric
  - plus - its strength, can be used to establish a secret between two parties
  - minus – expensive in terms of performance



- Symmetric
  - plus - less resource intensive
  - minus - requires key to be shared securely

Hashing



Hash Algorithm

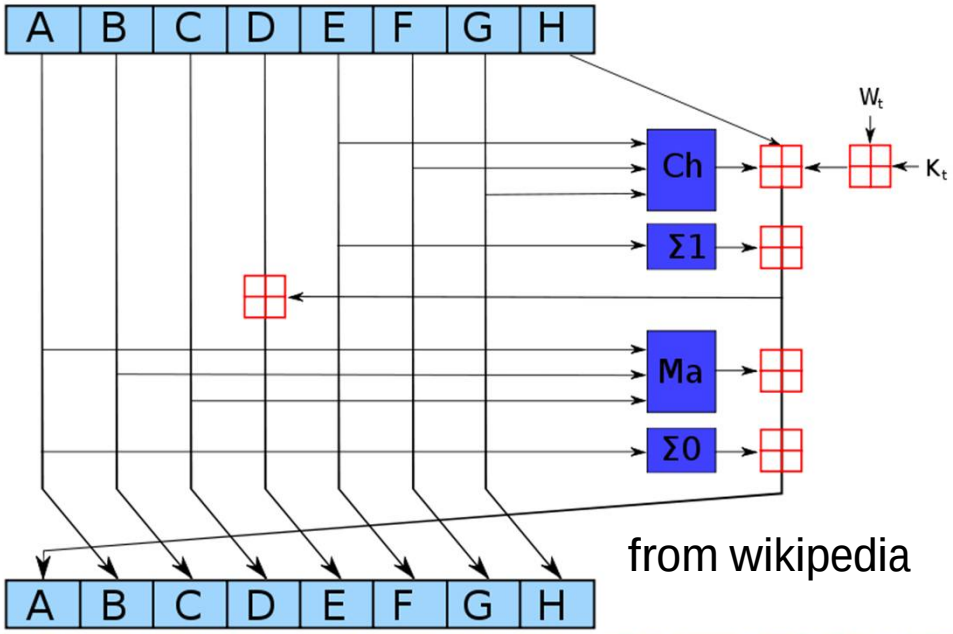
- Characteristics of a good hash algorithm
  - One-way – can't recover the data from the hash
  - Hard to find collisions
  - The result does not reveal information about the input

Hashing

- One iteration in a SHA-2 family compression function. The blue components perform the following operations:

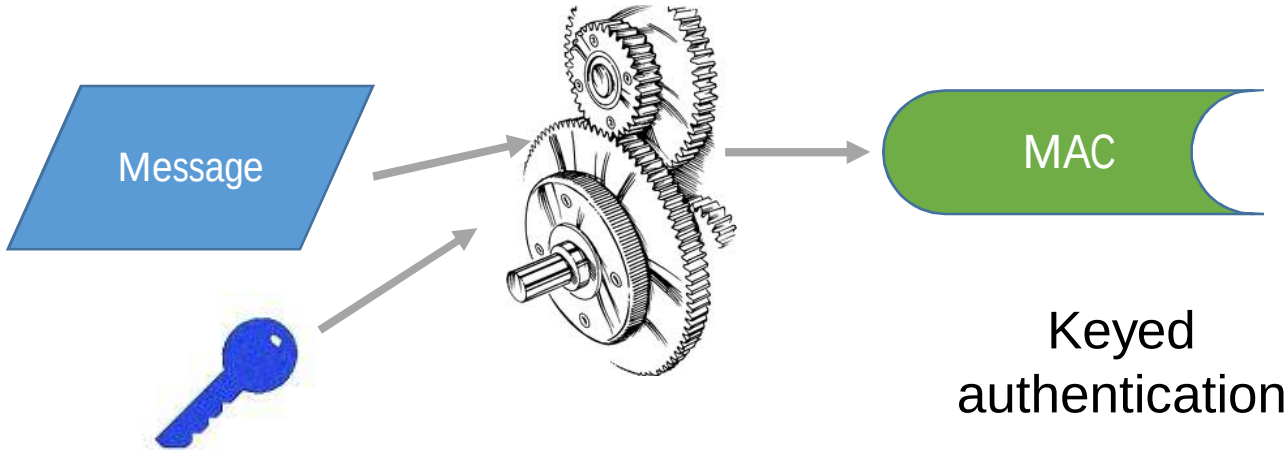
$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

- The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The red ⊞ is modulo 2^{32} addition.

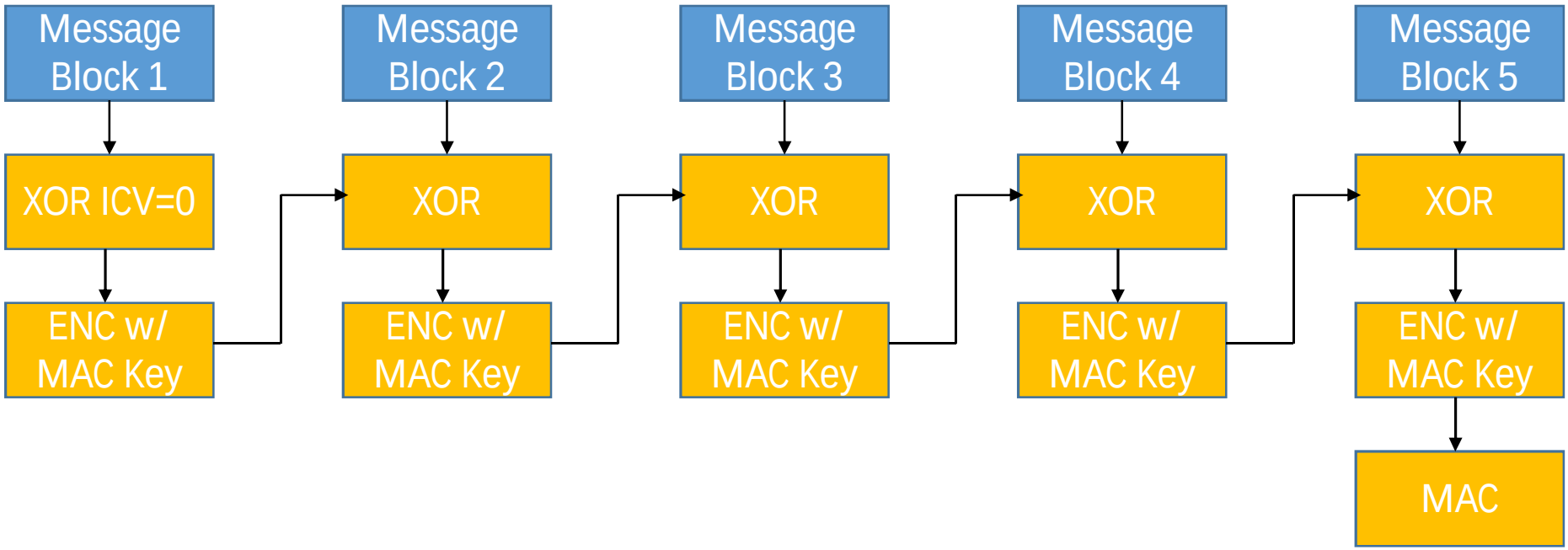


from wikipedia

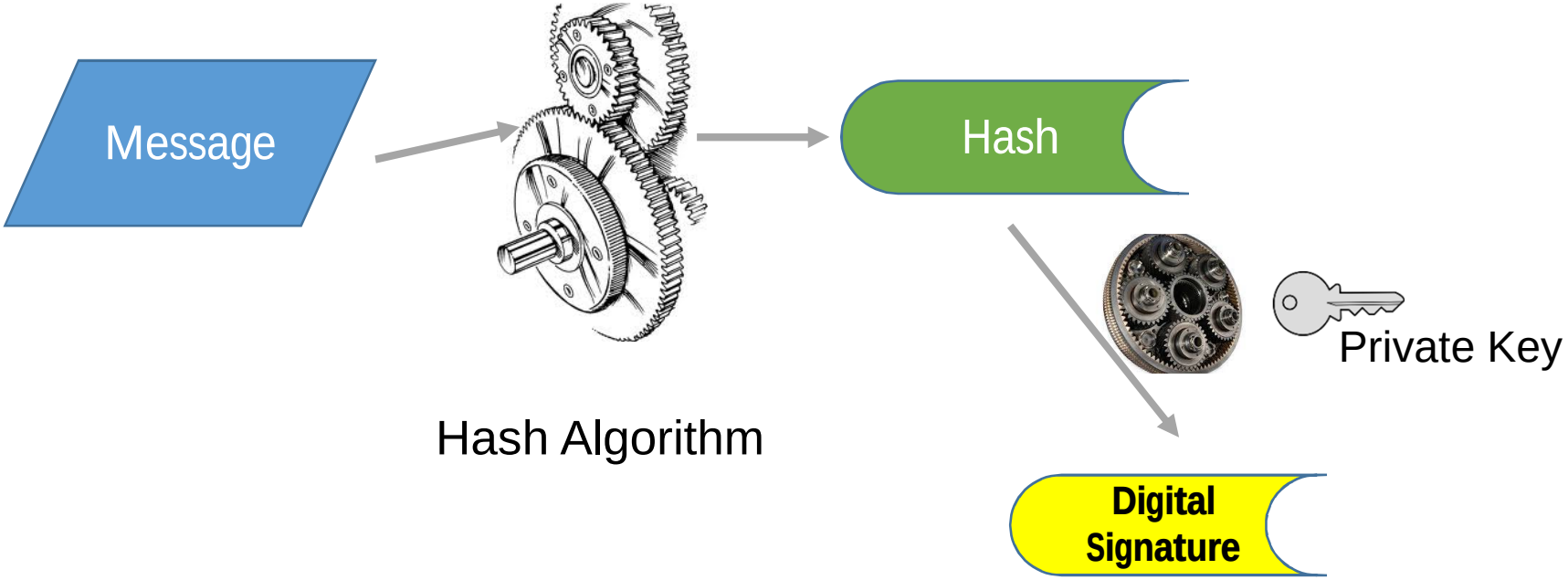
Hashing – Message Authentication Code

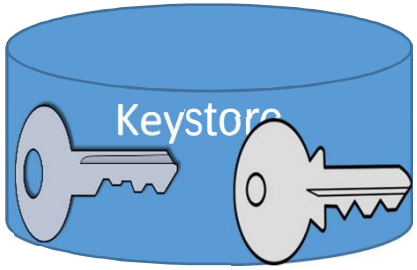


Keyed authentication



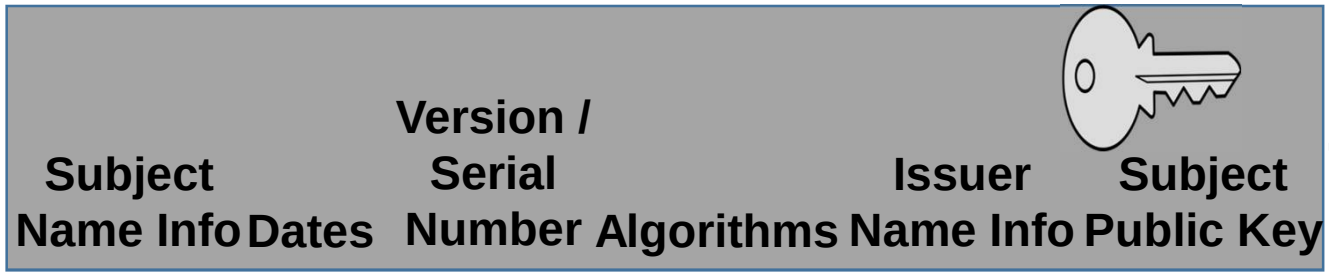
Digital Signatures

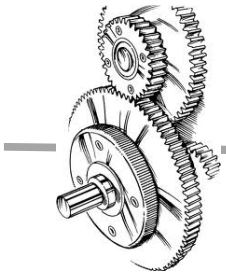




Certificates

Certificate Request



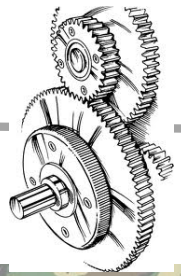


Hash

Certificate Authority Private Key

Digital Signature

Certificate



Hash

Certificate Authority Public Key

Financial Authentication - PINs

Routing Number:
12345678

Account Number: **9876543210**

Sequence Number: **1**

PIN Block:

4567898765432101

8A092F6E7D637B25

0925

Offset:
1234

2159

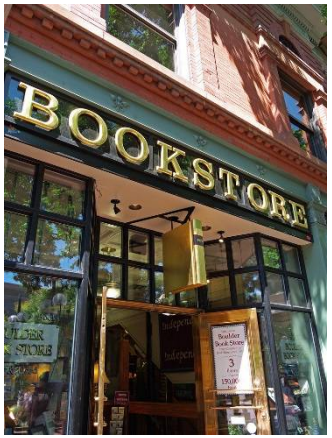
Pin Block Formats

ECI-2, ECI-3, ISO-0, ISO-1, ISO-2, ISO-3,

VISA-2, VISA-3, VISA-4, 3621, 3624, 4704-EPP

Decimalization Table			
0 -> 0	1 -> 1	2 -> 2	3 -> 3
4 -> 4	5 -> 5	6 -> 6	7 -> 7
8 -> 8	9 -> 9	A -> 0	B -> 1
C -> 2	D -> 3	E -> 4	F -> 5

References



- Cryptography Books
  - Bruce Schneier, “Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in ‘C’”, Addison Weley Longman, Inc. 1997
  - Simon Singh, “The Code Book”, Anchor Books, 1999
  - Niels Ferguson, Bruce Schneier, “Practical Cryptography”, Wiley Publishing, Inc. 2003
- Free Stuff
  - www.schneier.com – Bruce Schneier website, with monthly newsletter Cryptogram

Standards Doc

- RSA
  - PKCS #1 RSA Cryptography Specifications Version 2.2 (https://tools.ietf.org/html/rfc8017)
- ECC
  - https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
  - Also see 'Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
- AES
  - FIPS 197 Announcing the AES (https://doi.org/10.6028/NIST.FIPS.197)
- DES
  - FIPS 46-3 Data Encryption Standard - Withdrawn (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)
- TDES
  - SP 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final)

Questions …