SNIA NSF | NETWORKING STORAGE

Storage Networking Security Series: Encryption 101

Live Webcast

May 20, 2020

10:00 am PT

Today's Presenters

Ed Pullin
Product Line Marketing Manager
Intel® QuickAssist Technology

Judy Furlong
Distinguished Engineer
Dell Technologies

Alex McDonald
Vice Chair, SNIA NSF
NetApp

SNIA NSF | NETWORKING STORAGE

SNIA-At-A-Glance

SNIA. NSF | NETWORKING STORAGE

Technologies We Cover

- Ethernet
- iSCSI
- NVMe-oF
- InfiniBand
- Fibre Channel, FCoE
- Hyperconverged (HCI)
- Storage protocols (block, file, object)
- Virtualized storage
- Software-defined storage

SNIA NSF | NETWORKING STORAGE

SNIA NSF | NETWORKING STORAGE

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

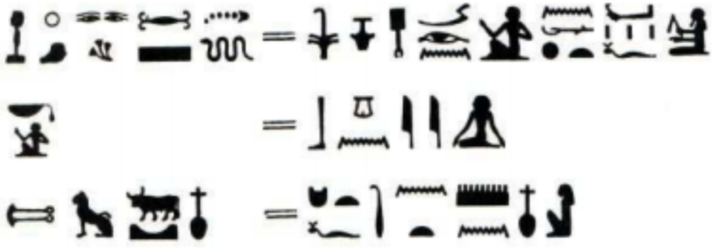
- Long History of Cryptography
- Security Basic Definitions – Cipher, Secret Keys, Entropy
- Precursors to Modern Cryptography
- Symmetric Cryptography - Cipher & Hash Details
- Asymmetric Cryptography - Public Key Crypto & Certificates
- Protecting Keys to The Realm - Key Management

Long History of Cryptography

7

Early Emergence of Cryptography

1. 1900 B.C. Ancient Egypt[1]



Substitution of unusual Hieroglyphic symbols to obscure the message meaning.
First Substitution Cipher.

2. 500 B.C. Ancient Sparta Scytale[2]

Transposition Cipher. Identical cylinders needed to align characters to recover message.

3. 56 A.D. Caesar Cipher[2]

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

Substitution Cipher. Encoding meant generally rotating letters to align with their substitution. Read with decoder ring.

1: http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf
2: http://www.cryptomuseum.com/crypto/caesar/cipher.htm

SNIA. NSF | NETWORKING STORAGE

Security Basic Definition

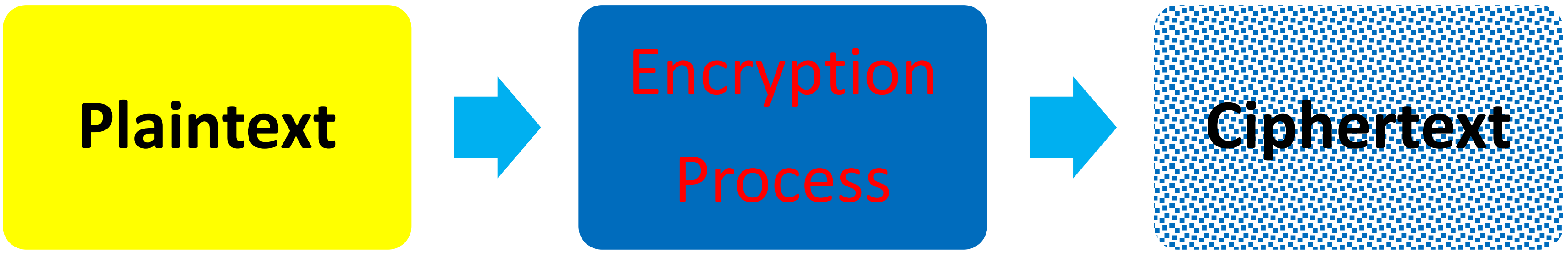
9

Security Basics - Cipher

Cipher

Cipher[1]

a: a method of transforming a text in order to conceal its meaning



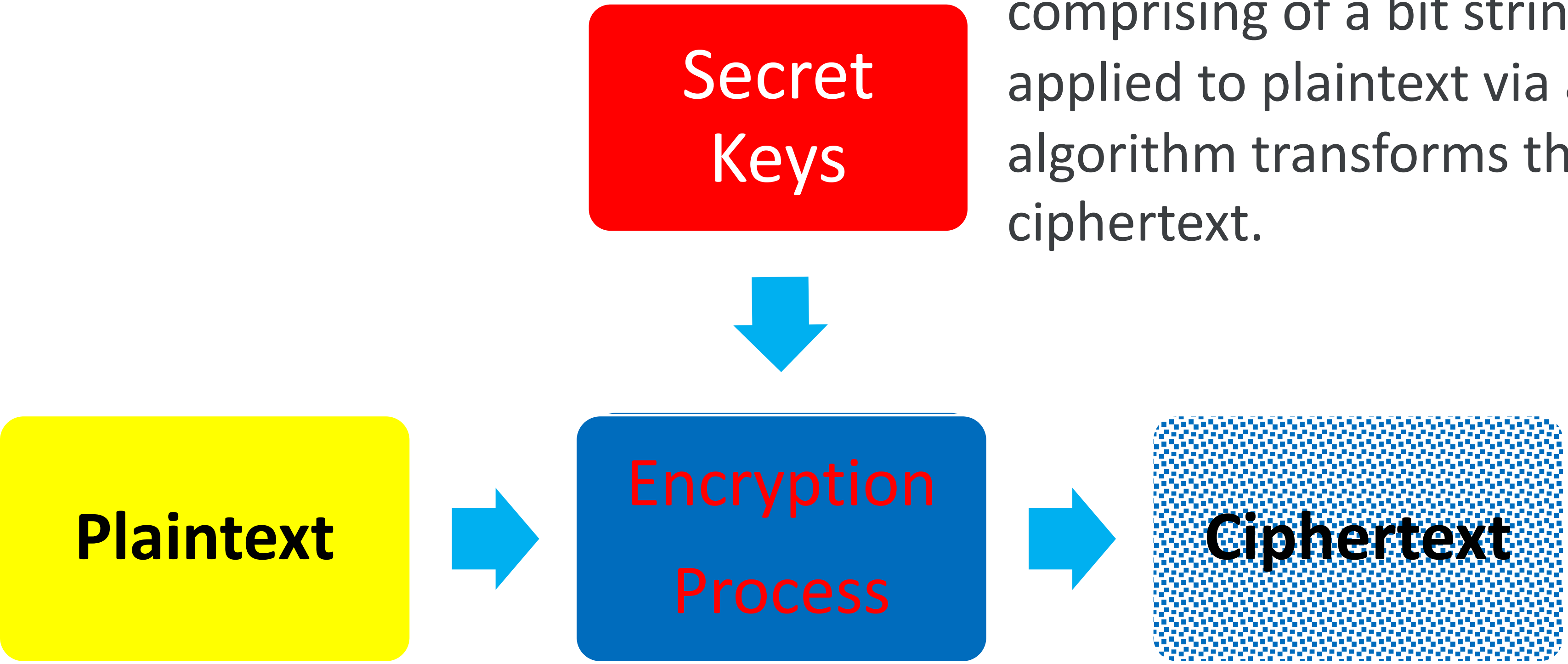
1: https://www.merriam-webster.com/dictionary

Security Basics – Secret Keys

Secret Cryptographic Keys

Secret Cryptographic Key[1]

a: Fundamental element in cryptography comprising of a bit string that when applied to plaintext via a cryptographic algorithm transforms the plaintext to ciphertext.



1: Intel Network Products Group Definition

Security Basics – Entropy

Entropy

Entropy (Noise) → True Random Numer Gen (TRNG) → Secret Keys

Plaintext → Encryption Process → Ciphertext

Entropy[1,2]

a: Chaos, Disorganization, Randomness.

b: Measure of the randomness of a data generating function.

Thermodynamic concept measuring disorder of a system, adapted by Claude Shannon in 1948 to describe the unpredictability of information.

1: https://www.merriam-webster.com/dictionary

2: https://www.sciencedirect.com/topics/computer-science/entropy

Precursors to Modern Cryptography

13

SNIA NSF | NETWORKING STORAGE

Precursors to Modern Cryptography

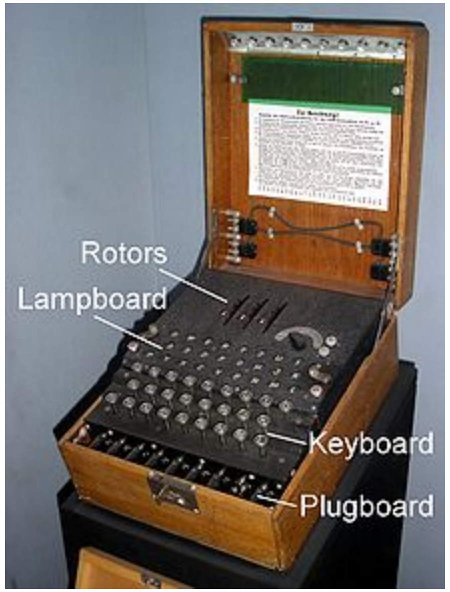
1. 1500 A.D Vigenere Cipher[1]

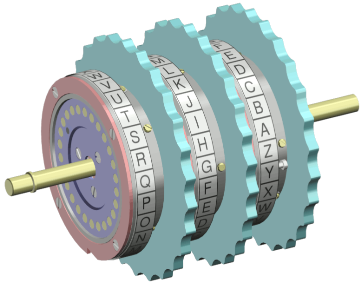
Plaintext		S	T	A	Y	S	A	F	E
Keyword		S	T	A	Y	H	O	M	E
Cipher Text		K	M	A	W	Z	O	R	I

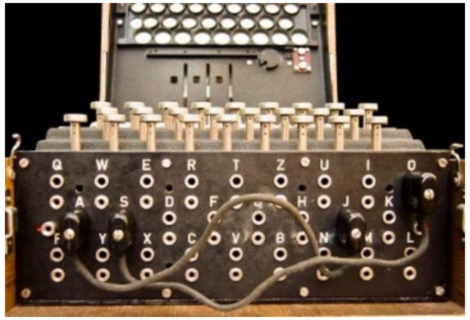
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Series of Caesar Ciphers with a keyword of same length as cipher used to align each new substitution.

2. 1920 A.D. Enigma[2]







Polyalphabetic settings with rotors and plug board settings. 150 Trillion ways that letters could be interchanged. Famously solved by Bletchley Park Government Code & Cipher School.

1: http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf
2: https://en.wikipedia.org/wiki/Enigma_machine

Symmetric Cryptography Cipher & Hash Details

15

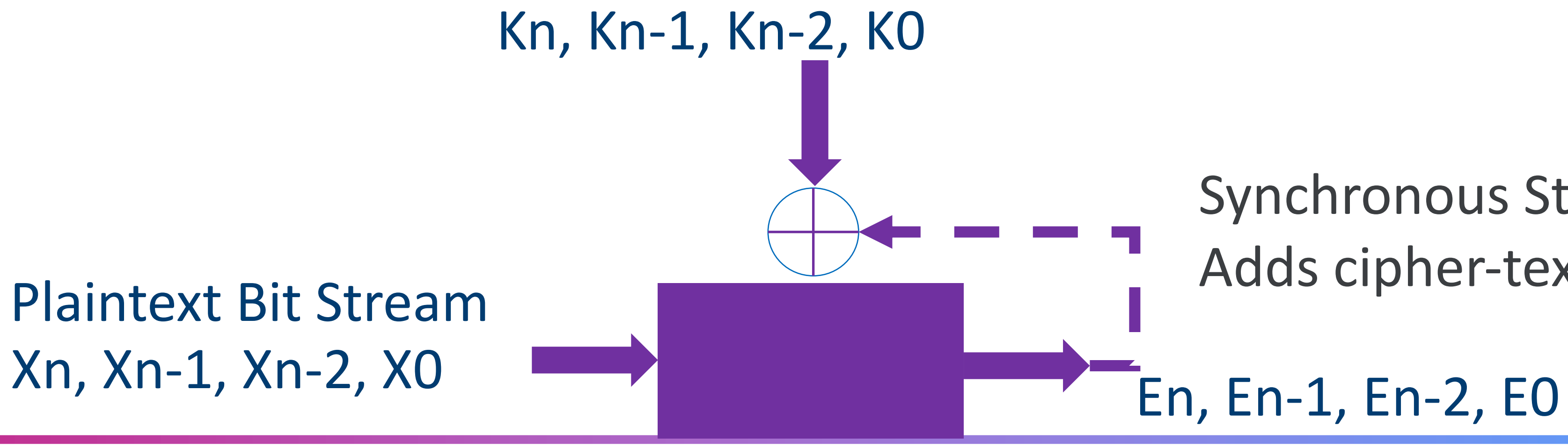
Bit for Bit

Stream Ciphers

Stream Ciphers[1]

a: Adding a bit from a key stream to a plaintext bit.

Rivest Cipher 4(RC4) was a popular stream cipher



Synchronous Stream Ciphers

Adds cipher-text feedback to key

1:Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verlag

Block at a Time

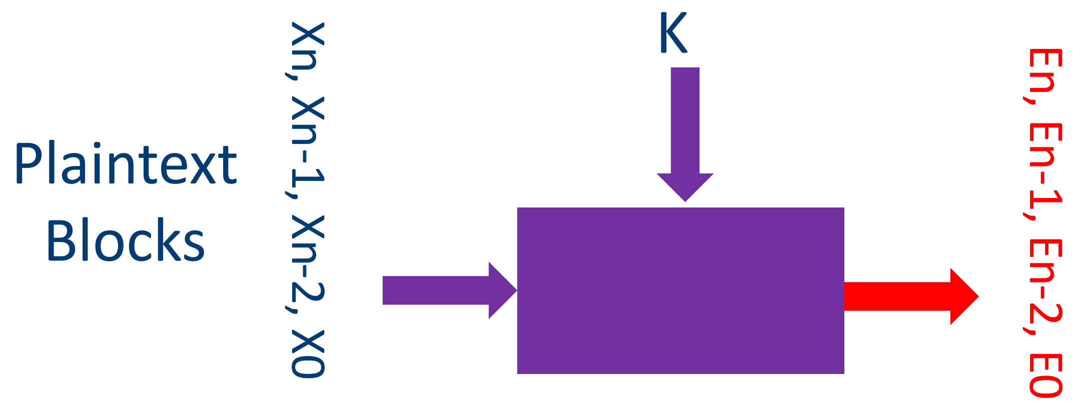
Block Ciphers

Block Ciphers[1]

a: Encrypt an entire block of data at a time with one key.

Encryption of bits in a block depends on other bits in a block.

Most common block is 128 bit(16 Bytes) for algorithms such as the AES Cipher



1:Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verlag

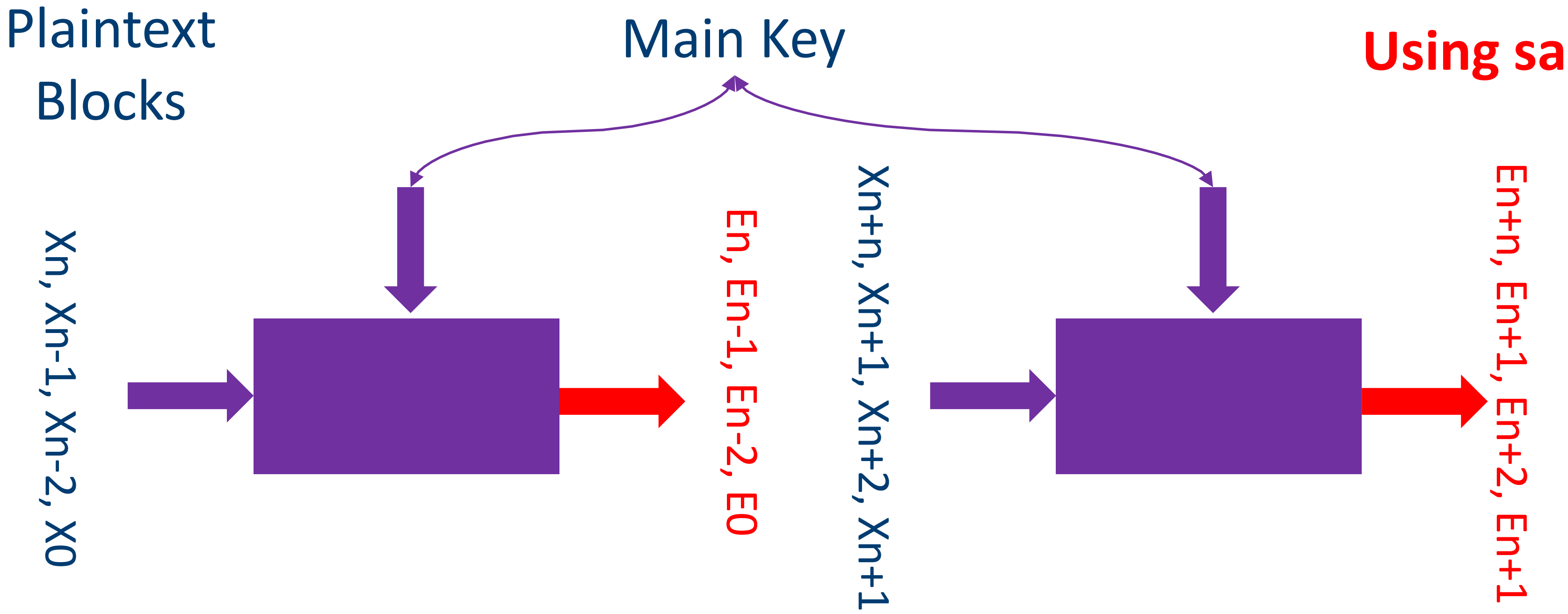
SNIA. NSF | NETWORKING STORAGE

Plug Information Leaks – Never Use Same Key

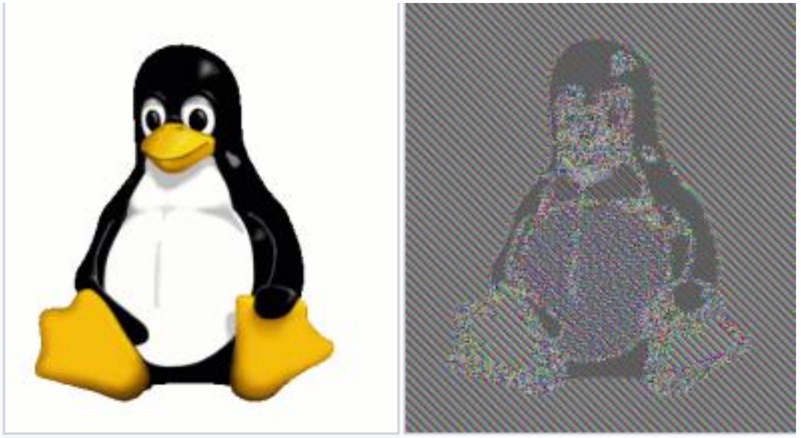
Leaking Detailed Information

ECB(Electronic Code Book) Mode[1]

a: Message is divided into blocks and each encoded separately



Using same key leaks information



Original image — Encrypted using ECB mode

1: Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verlag
2: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

SNIA. NSF | NETWORKING STORAGE

Encryption Must be Reversible

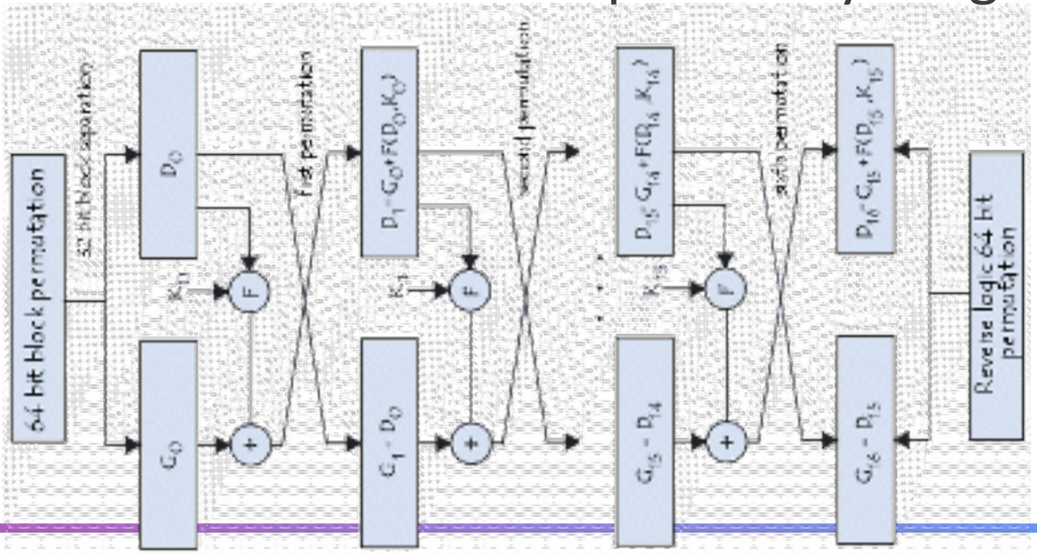
Encrypt ⟷ Decrypt

Ciphers must provide methods to go from plaintext to cipher-text and reverse that to go from cipher-text to plaintext

a. Example DES Block Algorithm with 56 Bit Keys published in 1976, later found to have key search & other analytic vulnerabilities – after vulnerabilities were exposed -3DES cascades this implementation 3 times and expands key usage[1]

Plaintext Blocks

X63 - X0



E63 – E0

 |

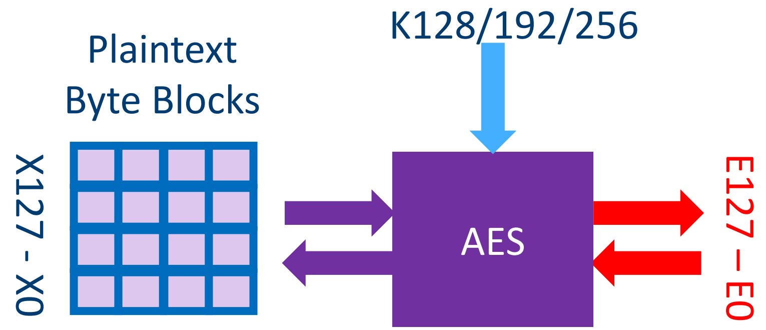
1: http://ccm.net/contents/134-introduction-to-encryption-with-des

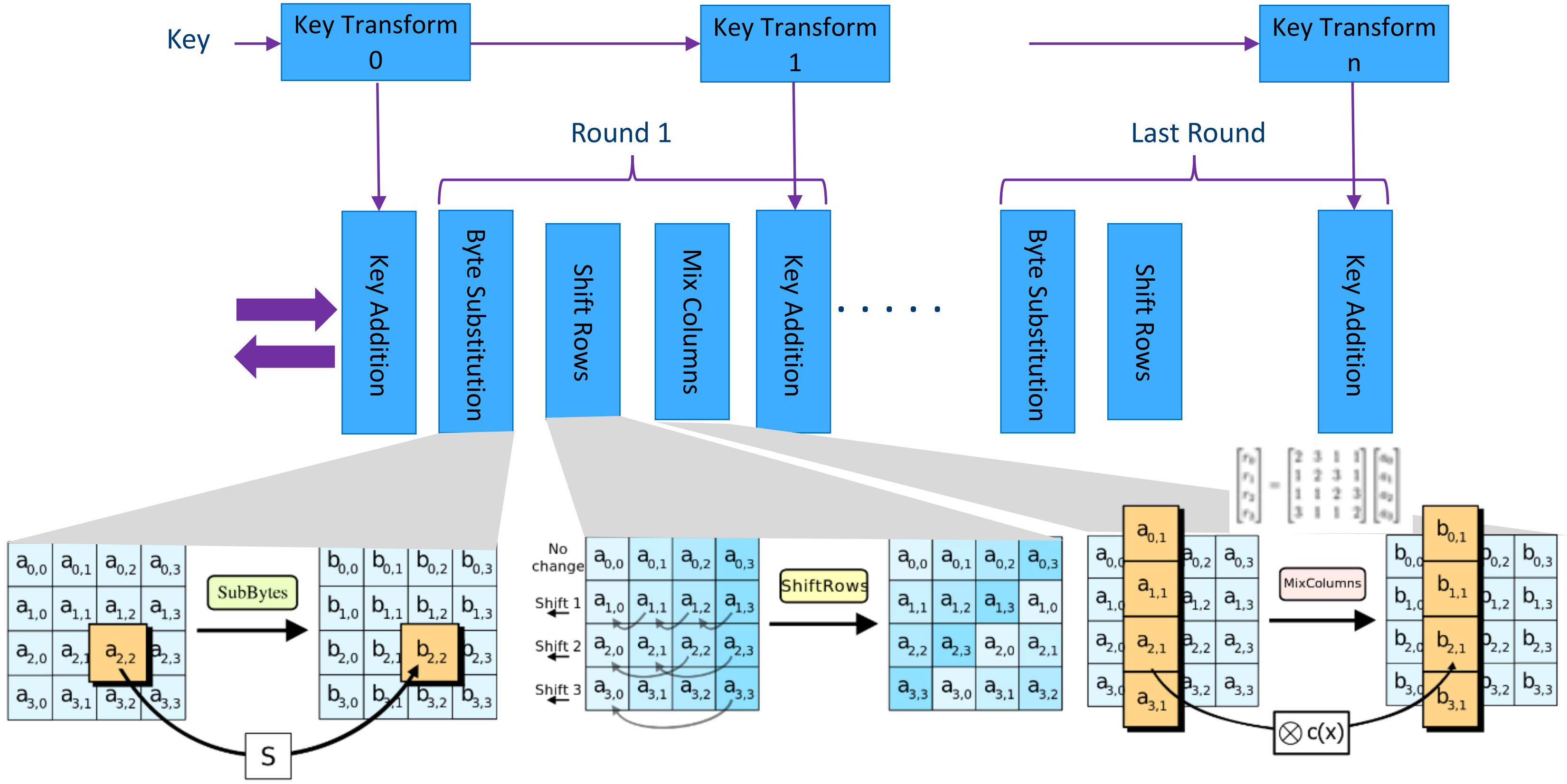
SNIA NSF | NETWORKING STORAGE

The Advanced Encryption Standard

AES

AES selected by NIST in 2001 after it's call for proposals for an Advanced Encryption Standard after weaknesses exposed in DES & 3DES. DES & 3DES implementations were not very efficient in Software. AES supports a block size of 128bits(16 Bytes). The algorithm can support 10, 12, or 14 rounds depending on the key selection.





1: Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verlag
2: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

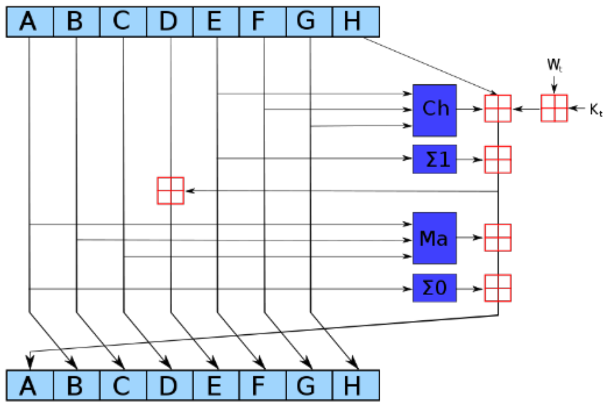
Hashing/Message Authentication

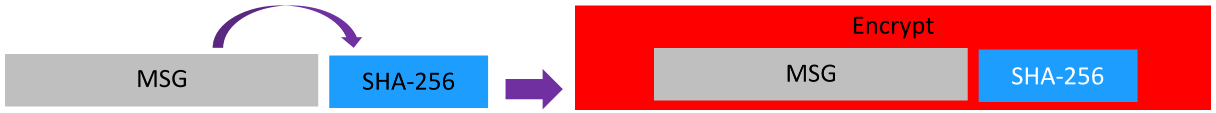
Modes of Operation

Hashes/Message Authentication compute a digest(unique fingerprint) of a message to act as digital signatures or authentication schemes to ensure message integrity.

A priority of hash schemes is strong collision resistance i.e. it is computationally infeasible to find 2 different inputs to produce the same hash.

SHA-1 was recently shown to not qualify as computationally infeasible and calls have gone out for the sun-setting of this hash for several years. Urgency now for industry to move to SHA-256(SHA-2)





SSL/TLS - MAC First then encrypt

IPSec – Encrypts Then MAC

This is always more secure

1: Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verlag
2: https://en.wikipedia.org/wiki/SHA-2

SNIA. NSF | NETWORKING STORAGE

Asymmetric Cryptography
Public Key Crypto & Certificates

22

Public Key Cryptography

Modes of Operation

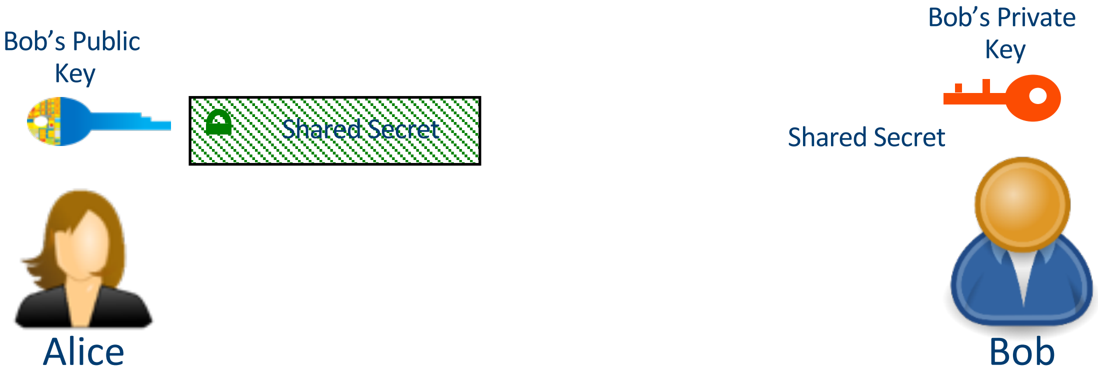
Is a form of Asymmetric Cryptography, because the Encryption Key is not the same as the Key for Decrypt.

The key used to Encrypt a Shared Secret is publicly known while the key used to decrypt that Shared Secret is held private and never disclosed.

The relationship between Public and Private keys is a mathematical relationship that makes it extremely infeasible to calculate one key from the other or expose the shared secret.

One common Public Key Cryptography method is the RSA – Named after Rivest, Shamir & Adleman, based on Modular Exponentials and Prime Number relationships. The mathematics is based on Fermat & Eulers prime modulo from the 17th & 18th Centuries. A second common method is Elliptic Curve Cryptography based on intersections on elliptic curves of the form

$y^2 = x^3 + ax + b \bmod (primep)$



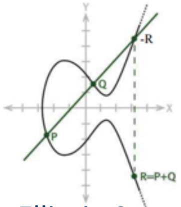
Alice Encrypts a Shared Secret with Bob's Public Key

Bob Decrypts with his Private Key

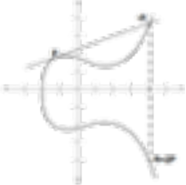
Now each can encrypt/decrypt using the Shared Secret

Secret^(epub*dpvt) => x^ 1 mod(PHI(N)) => x^((any integer)*PHI(N) + 1) => ***Secret***

RSA Using Modular Exponentials



Elliptic Curve Point Addition



Elliptic Curve Point Multiplication

dPrivate*P = T(Public)

1: Adams, Carlisle, Lloyd, Steve 1999, Understanding PKI 2nd Edition, Addison-Wesley
2: Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verla

SNIA. NSF | NETWORKING STORAGE

Public Key Infrastructure - Certificates

Using Certificates & Establishing Trust[1]

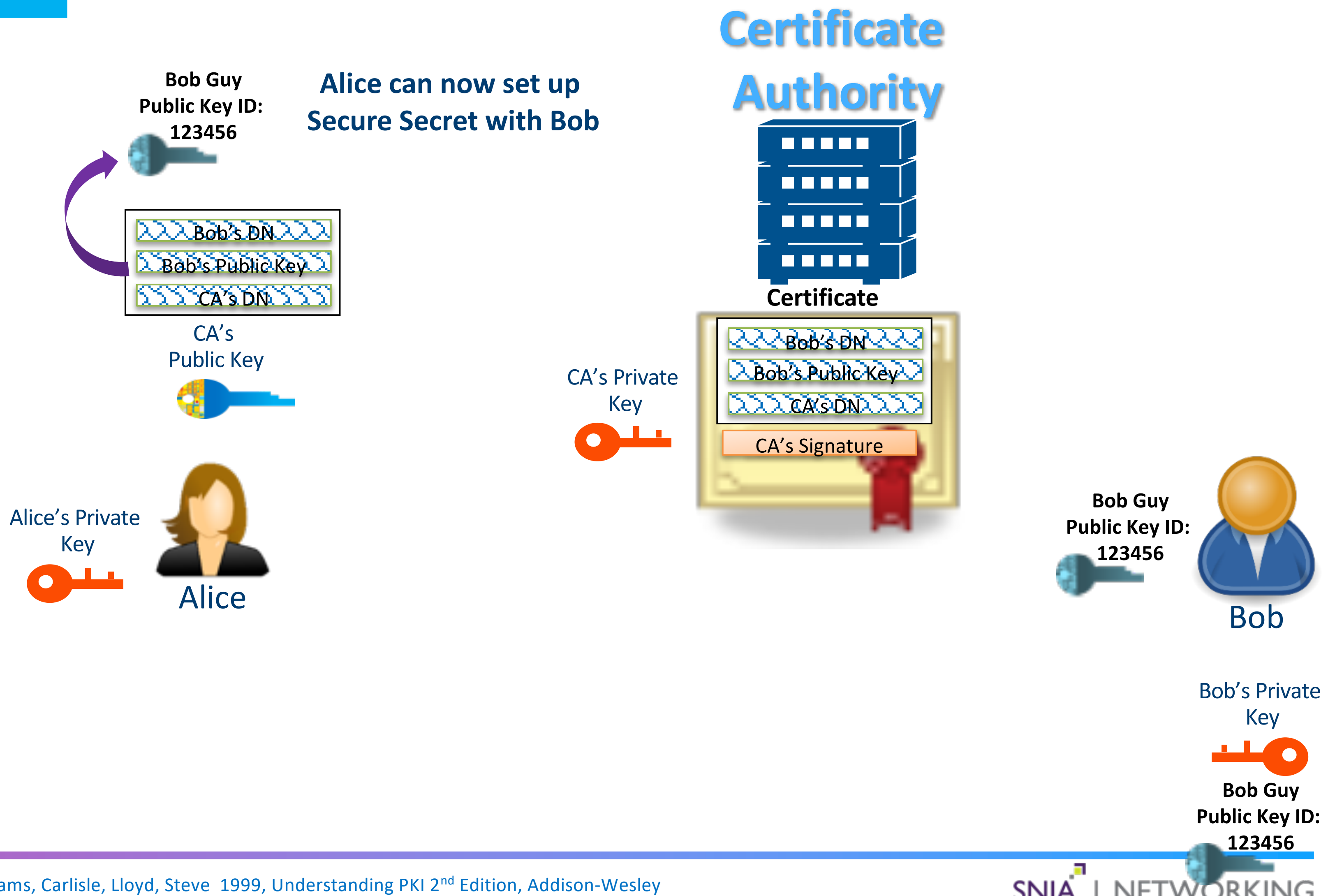
A certificate Authority is an entity that allows us to establish trust. The Certificate Authority certifies the key & identity by providing a trusted digital signature over them.

Bob can send his ID credentials & Public Key, which is then signed by the certificate Authority using its Private Key.

The Authority then gives Bob his signed Certificate binding his ID & Public Key.

To start communication bob can then send his signed certificate.

Alice can use the CA's Public Key to decrypt the CA and retrieve Bob's Public Key which can be verified to be the public Key that is being used for the session.



1: Adams, Carlisle, Lloyd, Steve 1999, Understanding PKI 2nd Edition, Addison-Wesley
2: Paar, Christof, Pelzel, Jan, 2010, Understanding Cryptography , Berlin Heidelberg, Springer-Verla

SNIA. NSF | NETWORKING STORAGE

Protecting the Keys to the Realm
Key Management

SNIA NSF | NETWORKING STORAGE

Key Management

- Keys make cryptographic functions unique
- Key management focuses on protecting keys from threats and ensuring that keys are available when needed
- Different approaches are taken for managing symmetric and asymmetric keys
- Key management needs to seamless integrate with the deployment model and architecture of a cryptographic capable application/product

Encryption 101 Conclusion

27

SNIA NSF | NETWORKING STORAGE

Conclusion

- History of cryptography is expansive, and filled with fundamental learnings that lead to the discipline's constant and necessary evolution.
- Symmetric Cryptography consists of reversible cipher algorithms & modes. Symmetric Cryptography algorithms use the same secret keys for encryption & decryption.
- Hashing & Message Authentication provides a unique fingerprint over the data that can be used as a data integrity check or unique data handle for storage.
- Asymmetric Crypto uses a public/private key pair, one for encrypt & its pair for decrypt. It forms the basis of our ability to broadly communicate securely and provides for Certificate root of trust management.
- Key Management: Protecting keys is absolutely critical to protecting information!

SNIA. NSF | NETWORKING STORAGE

The Storage Networking Security Webcast Series

On-demand at the SNIA Educational Library: snia.org/educational-library

- Understanding Storage Security and Threats
- Securing Data at Rest – May 27, 2020
- Key Management 101 – June 10, 2020
- Follow us on Twitter @SNIANSF for dates and times of others planned:
  - Applied Cryptography
  - Protecting Data in Transit
  - Securing the Protocol
  - Security Regulations
  - Securing the System: Hardening Methods

After this Webcast

- Please rate this webcast and provide us with your feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast, including answers to questions we couldn’t get to today, will be posted on our blog at https://sniansfblog.org/
- Follow us on Twitter @SNIANSF

SNIA. NSF | NETWORKING STORAGE