Education

CRYPTOGRAPHY DECIPHERED!

Michael Willett
SAMSUNG

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- 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 Education Committee.
- 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.

Abstract

Cryptography Deciphered!

Cryptography, the science of "secret writing", is being exploited more extensively by the I.T. community in order to provide data confidentiality and to satisfy multiple regulatory requirements. Cryptography is also a component in other elements of the security infrastructure, including authentication/authorization, identity management, data integrity, and non-repudiation. Cryptographic methods and associated best practices are essential elements of a successful, modern business. Cryptography comes in two flavors: symmetric cryptography for high-speed and bulk encryption, asymmetric (or public-key) cryptography for instantaneous, shorter, yet secure encryption. The state-of-the-art cryptography standards and methods for both flavors will be reviewed, with a eye toward how each technology is integrated into an overall I.T. strategy. A brief, historical perspective on cryptography will be included. Advanced level of depth.

Learning objectives:

Understand the basic algorithms of cryptography, both symmetric and asymmetric
Appreciate the role of cryptography in the overall security infrastructure
Learn how cryptography helps satisfy business objectives

You probably have read about….

- A lot of storage security product announcements addressed at preventing repeats of past data "indiscretions" (data breaches)
  - Fueled by "lost tapes" & "lost laptop" scenarios
- A lot of confusion about data "in-flight" versus data "at-rest" security (see the SNIA Dictionary[1])
- Issues with keys & related difficulties
  - Human involvement (e.g. policy creation, cross-group interaction): the source of much difficulty

SNIA Tutorial:

ABCs of Encryption

1. http://www.snia.org/education/dictionary/

CPGP1RTRH0YOAY1

C P G P 1

R T R H 0

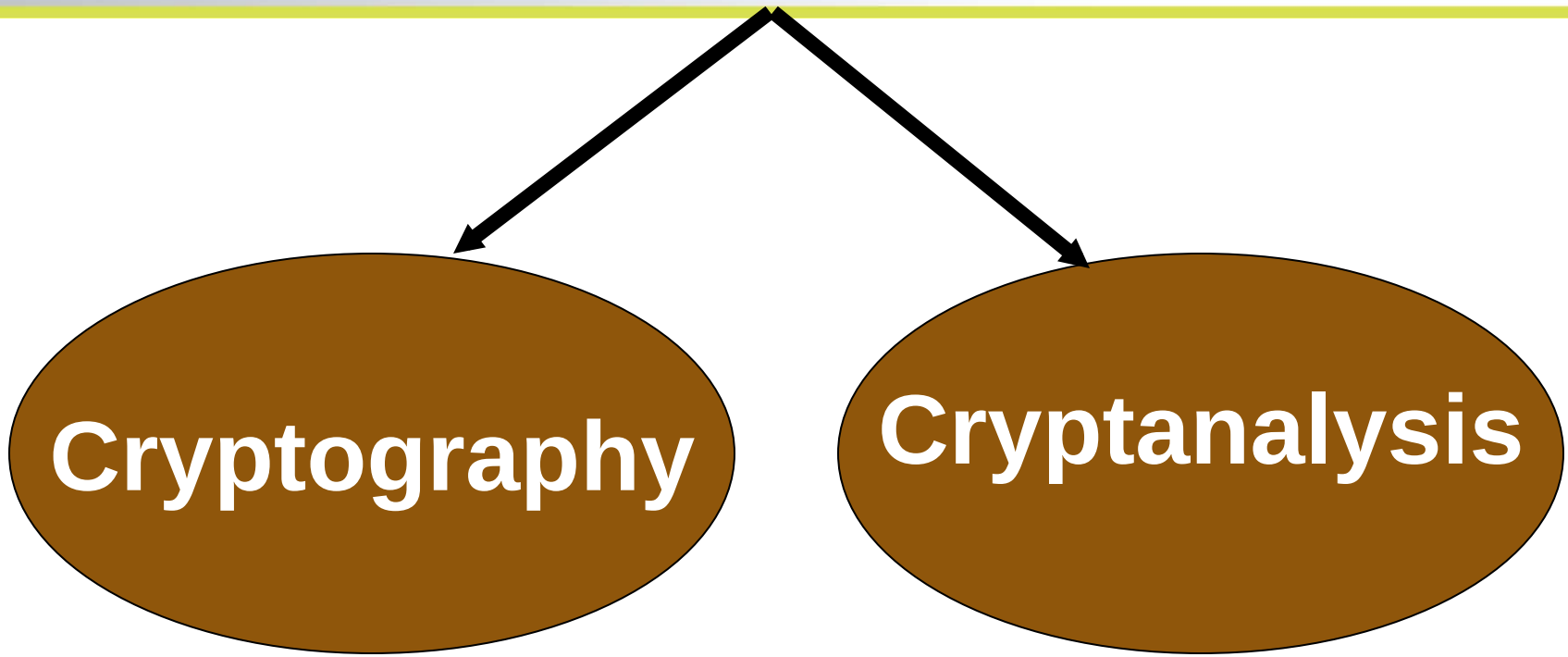
Y O A Y 1

CRYPTOGRAPHY101

Transposition Cipher

"STIRRING"

CRYPTOLOGY



Code Making

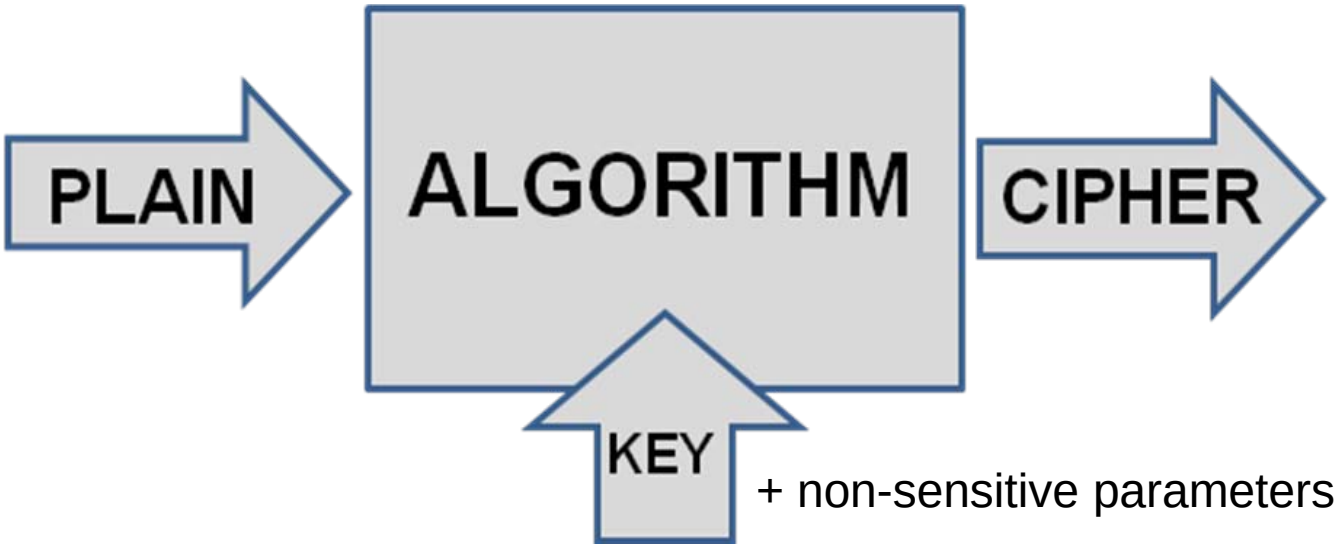
Code Breaking

EXAMPLE

CryptoQuotes

English statistics

Cryptography Ingredients

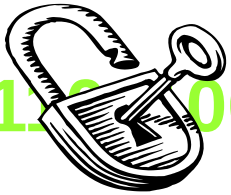


"Strength" of the cryptographic system:

- **ALGORITHM produces "random-looking" CIPHER from any PLAIN**
  Determined through exhaustive analysis and mathematical proof
- **Difficulty of guessing or re-producing the KEY**
  large key space (= all possible keys)

Ex: 2^{128} possible 128-bit AES keys, which is about
340,000,000,000,000,000,000,000,000,000,000,000
"Exhaustive search" (or brute force attack): test all possible keys

Classical Cryptography



0110011[illegible]0010101

SECURE

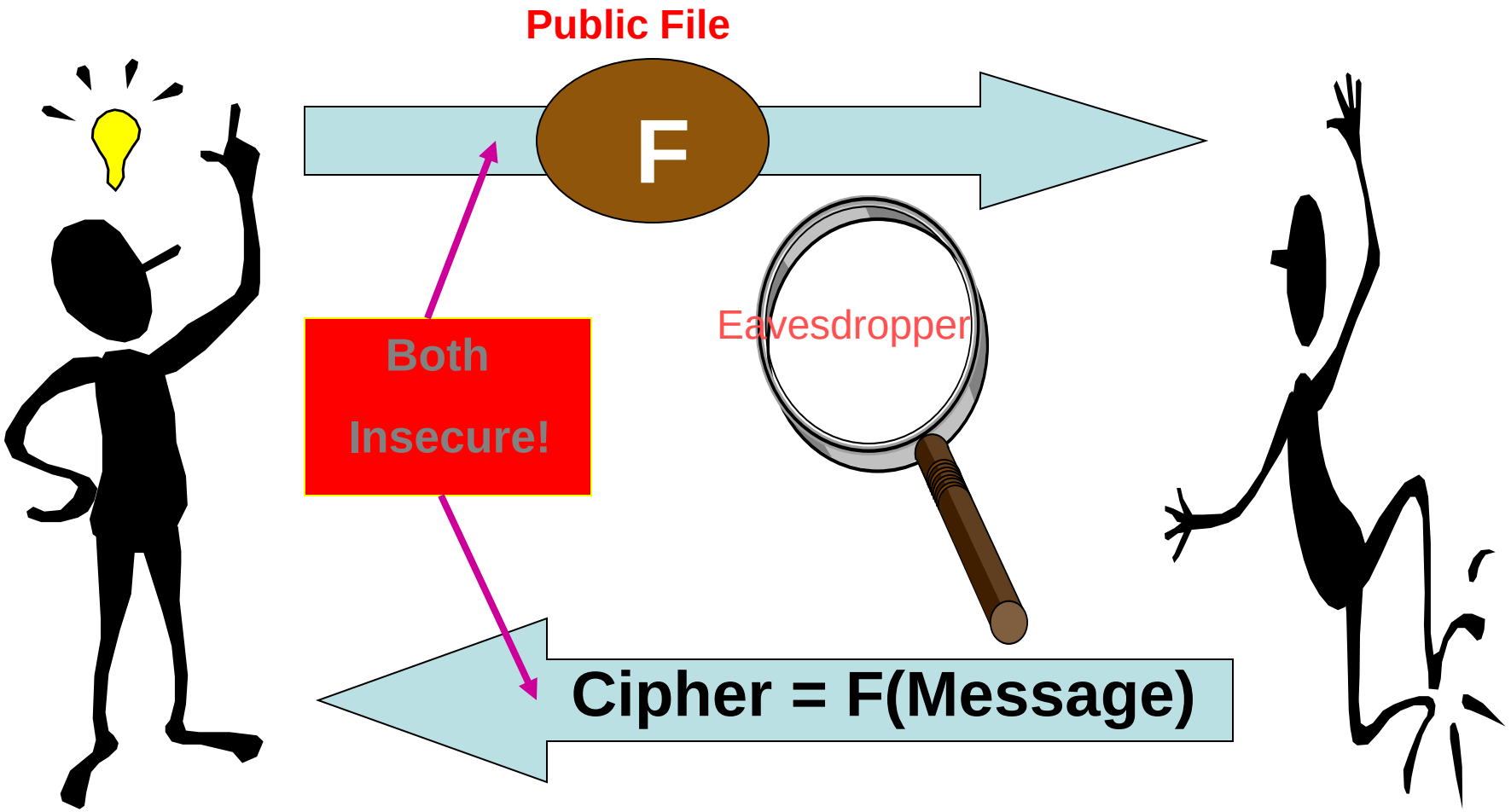
K Key Channel K

INSECURE

Cipher = Encode(Message, K)

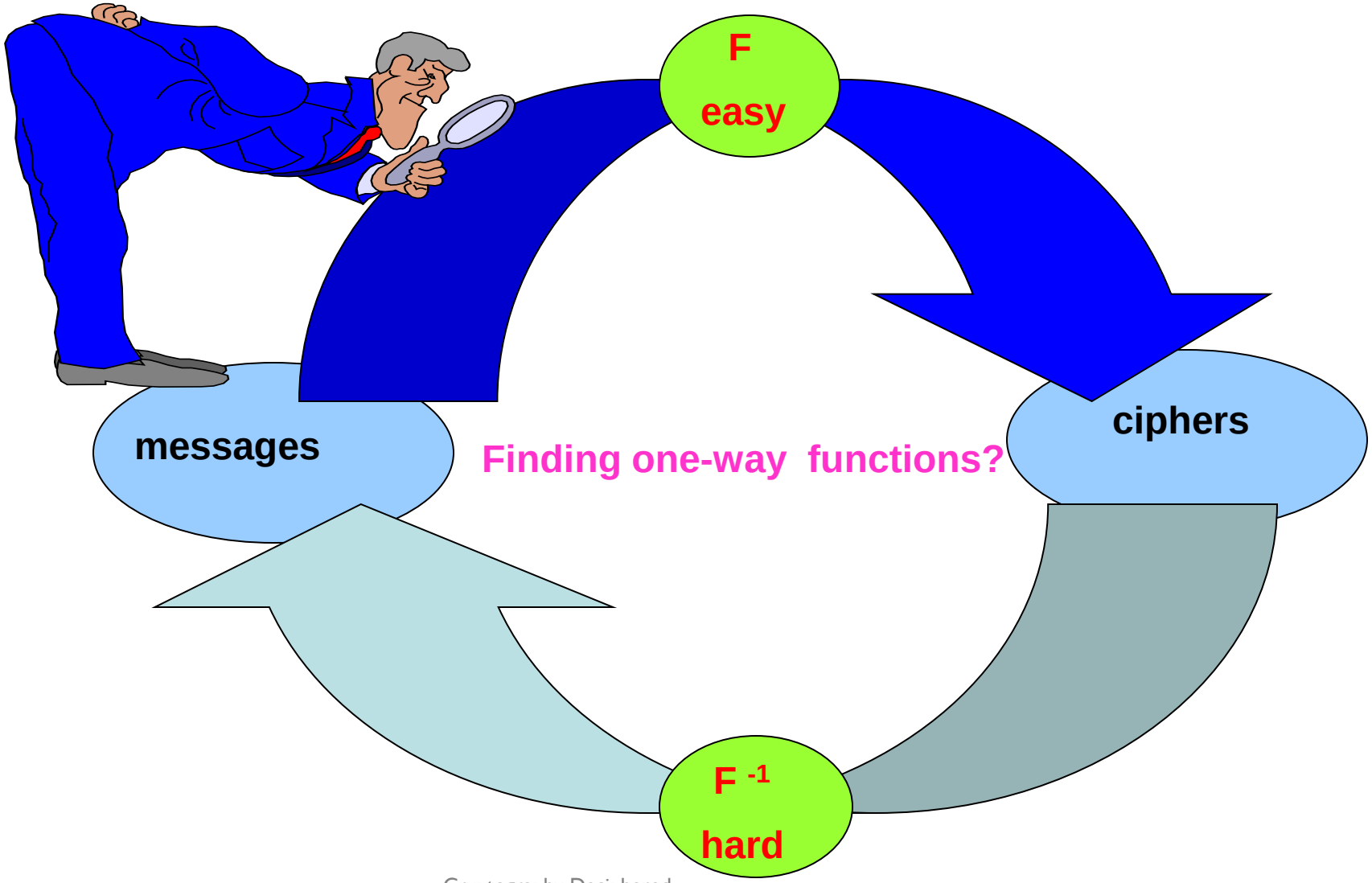
Eavesdropper

Public-Key Cryptography (1976[1])

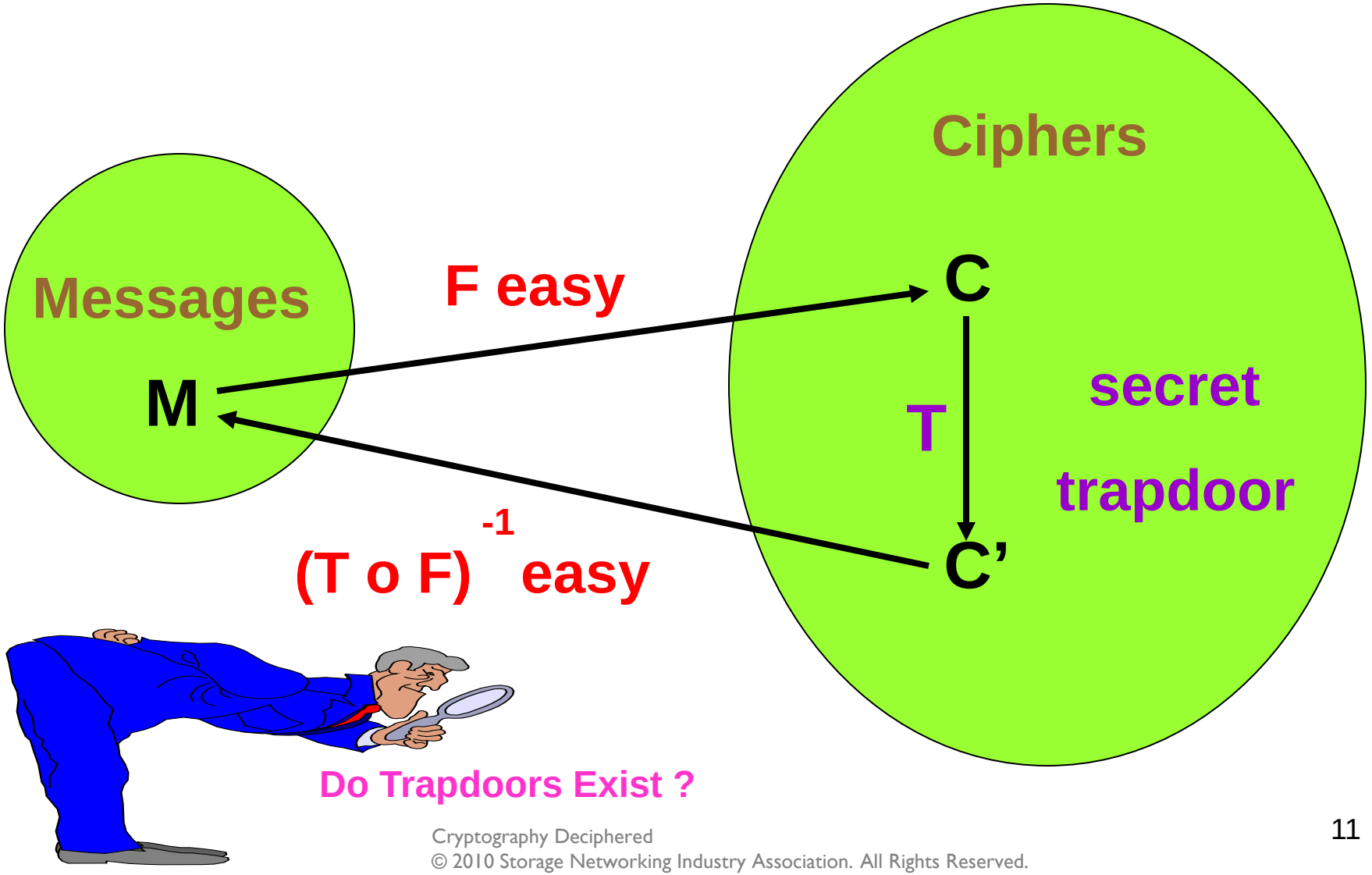


1: Actually, James Ellis (UK/CESG) circa 1970; kept SECRET until 1987!
http://web.archive.org/web/20030610193721/http://jya.com/ellisdoc.htm

One-Way Functions

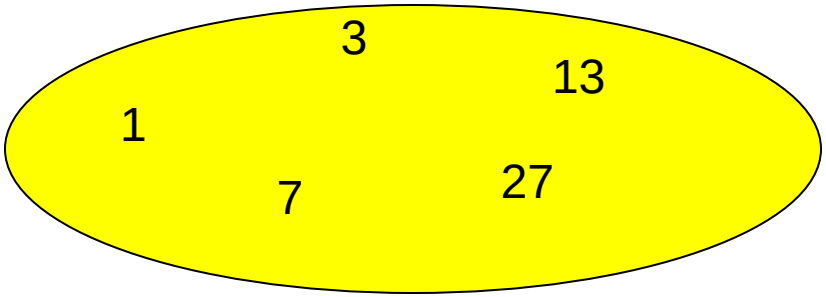


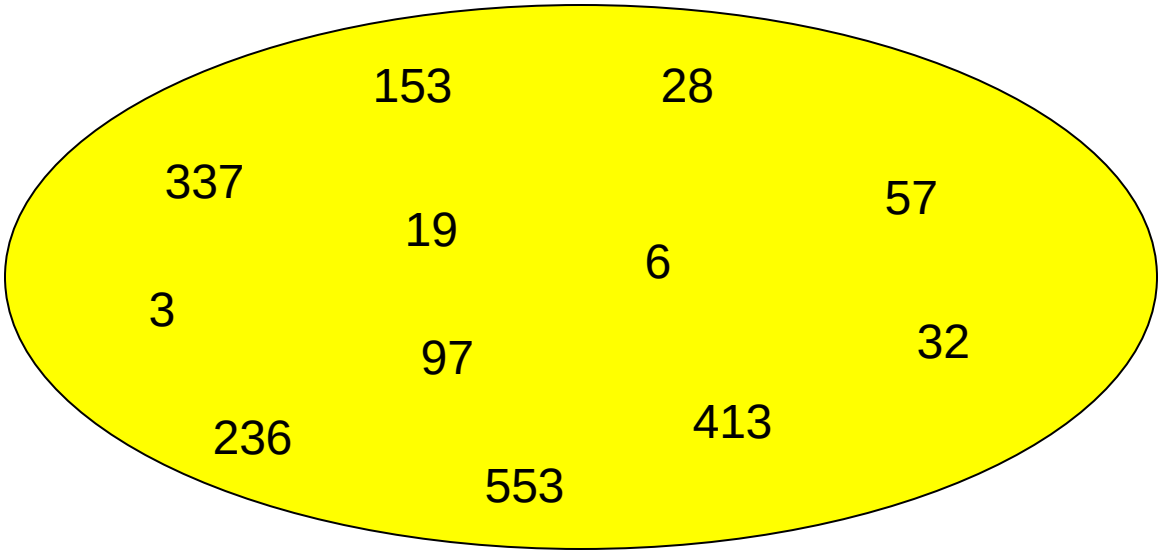
How Does Alice Decode Her Messages?



One-Way Functions

ADDITION





Proof of Hardness ?

Trapdoor ?

Target 4 11 40

Target 396

Knapsack Public-Key

Observation: Addition is easy to do, hard (???) to undo

Other One-Way Functions

Education SNIA

Multiply 1321 x 987 = 1303827 **easy**

Factor ??? x ??? = 971259 **hard ?**

Power 6^5 = 7776 **easy**

Root $(???)^5$ = 59049 **hard ?**

WAIT!! Powers are easy ?

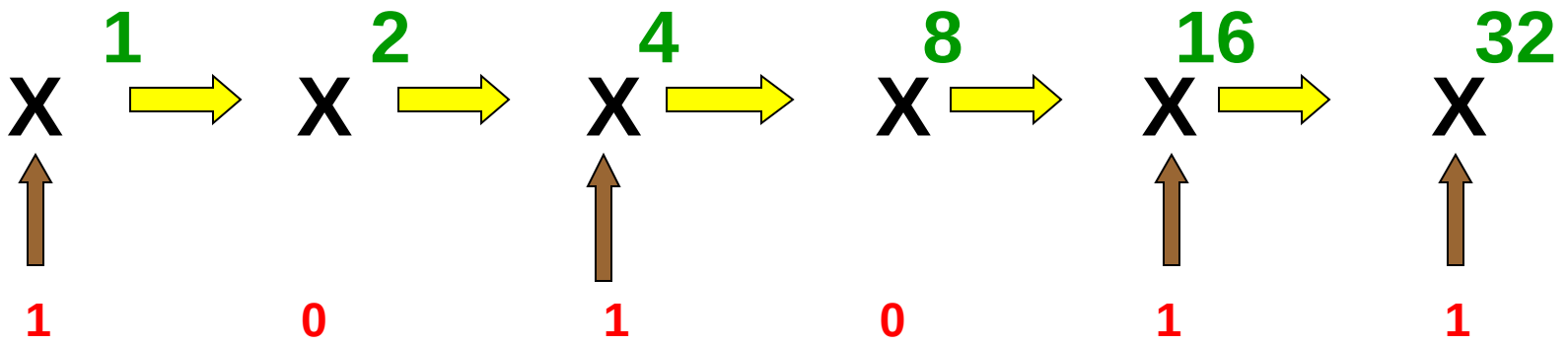
422191

3650502 = ???

Horner's Rule

$$x^{53} = ???$$

$$53 = 1 + 4 + 16 + 32 = 101011 \text{ in binary}$$



$$x^{53} = x^{1} \times x^{4} \times x^{16} \times x^{32}$$

Modular Arithmetic (tutorial)

$$R = K \bmod (N)$$

$$\begin{array}{r|l} & Q \\ \hline N & K \\ & \ldots \\ \hline & R \end{array}$$

$$K = N \times Q + R$$

discard

15 mod(7) = 1 31 mod(7) = 3 **53 x 17 = 1 mod(60)**

multiplicative inverses

Rivest-Shamir-Adleman (RSA)

Education SNIA

P = 7 Q = 11 primes

N = 7 x 11 = 77

(P - 1) x (Q - 1) = 6 x 10 = 60

FIND D x E = 53 x 17 = 1 mod(60) EASY!

$$\text{CIPHER} = (\text{MESSAGE})^{17} \bmod(77)$$

$$(\text{CIPHER})^{53} \bmod(77) = \text{MESSAGE}$$

MAGIC!

PUBLIC 17 N = 77 Secret Trapdoor 53 (or P=7 Q=11)

WAIT!!!

WHAT IS WRONG WITH

THIS PICTURE ??

RSA: "Pick two PRIMES of length 512 bits (or 1024, 2048, …) ?!? .... "

P is PRIME if its only factors are 1, P… try to FACTOR P hard!

How to Find Large Primes

Brute Force: Pick P at random, test all possible factors $0 < X < P$

TAKES FOREVER!!

Fermat's Theorem: IF P is prime, then

$$X^{P-1} = 1 \mod (P) \text{ for } 0 < X < P \text{ (test)}$$

Fact: (test) is true for ALL X if and only if P is prime (rare exceptions)

EASY TO (test) ONE X, BUT USELESS FOR ALL X

Neat fact: If P is NOT prime, then (test) FAILS for over half the X

Super test: Pick P at random. Sample T random values of X

IF (test) is TRUE for all T values of X, then

probability(P is NOT prime) $< (1/2)^{T}$ (VERY small!!!)

Digital Signatures

RSA: E, N public, D secret (P, Q destroyed!)

Genius!: REVERSE the order of use; ie, apply D first (only I can):

$$(\text{name.MESSAGE})^{D} \bmod(N) = \text{“signature”}\ \text{(gobbledygoop!)}$$

Anybody: calculate $(\text{“signature”})^{E} \bmod(N) = \text{name.MESSAGE}$

I can “sign” a MESSAGE:

name.MESSAGE || “signature” = certificate

- o is associated with ME
- o CANNOT be forged

SIGNATURE

Certification Authority (CA)

"Well known authority" chooses Public and Private Key

Choose my own Public and Private Key

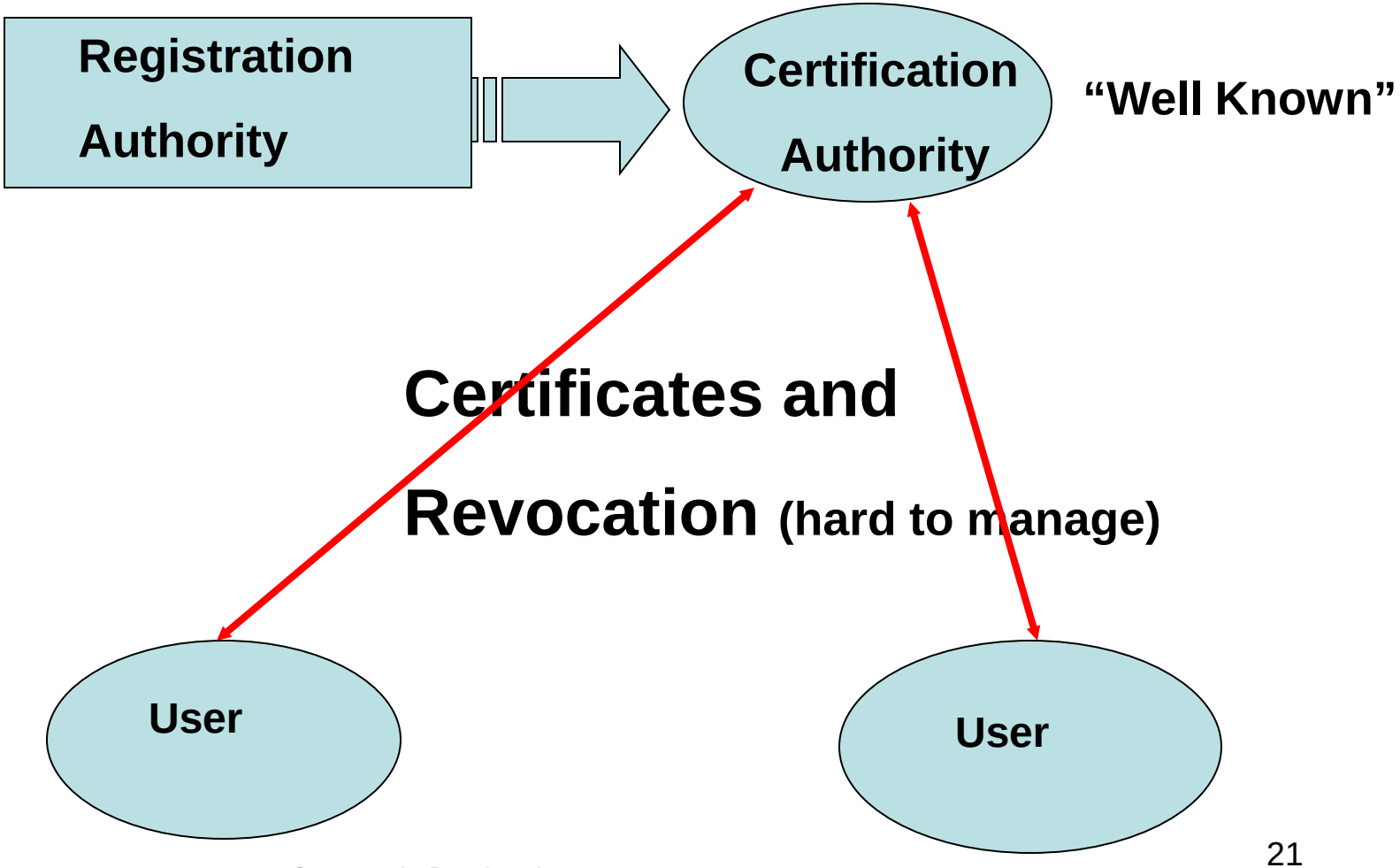
The CA authenticates me (ID) and then signs my public key:

my CERTIFICATE = ID.Public || Private (ID.Public)

When someone wants my Public Key, I (or anyone) sends my CERTIFICATE

Check certificate signature by applying well-known CA Public Key

Public Key Infrastructure (PKI)

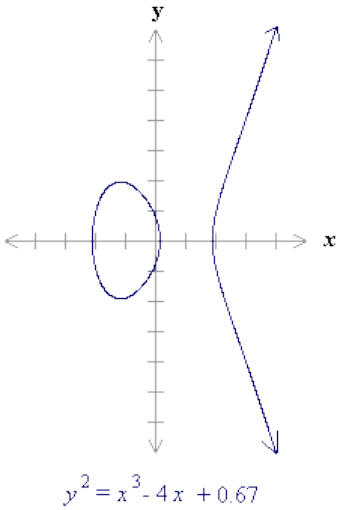


Elliptic Curve Cryptography

Recall: Equation for a circle centered at (a,b) of radius r:

(x-a)^2 + (y-b)^2 = r^2

An **elliptic curve** is also defined by an equation, but it has the slightly more complicated form; example:



y^2 + x·y = x^3 + a·x^2 + b

Points (x,y) on the elliptic curve are the algebraic objects for elliptic curve cryptography, with addition and exponentiation defined by… (whoa! Let's stop here)!

FACTORING

State of the art: Number Field Sieve reduces the strength of public-key schemes over modulo integers, but not over elliptic curves.

Net: smaller bit-length elliptic curve can replace higher-bit modulo schemes

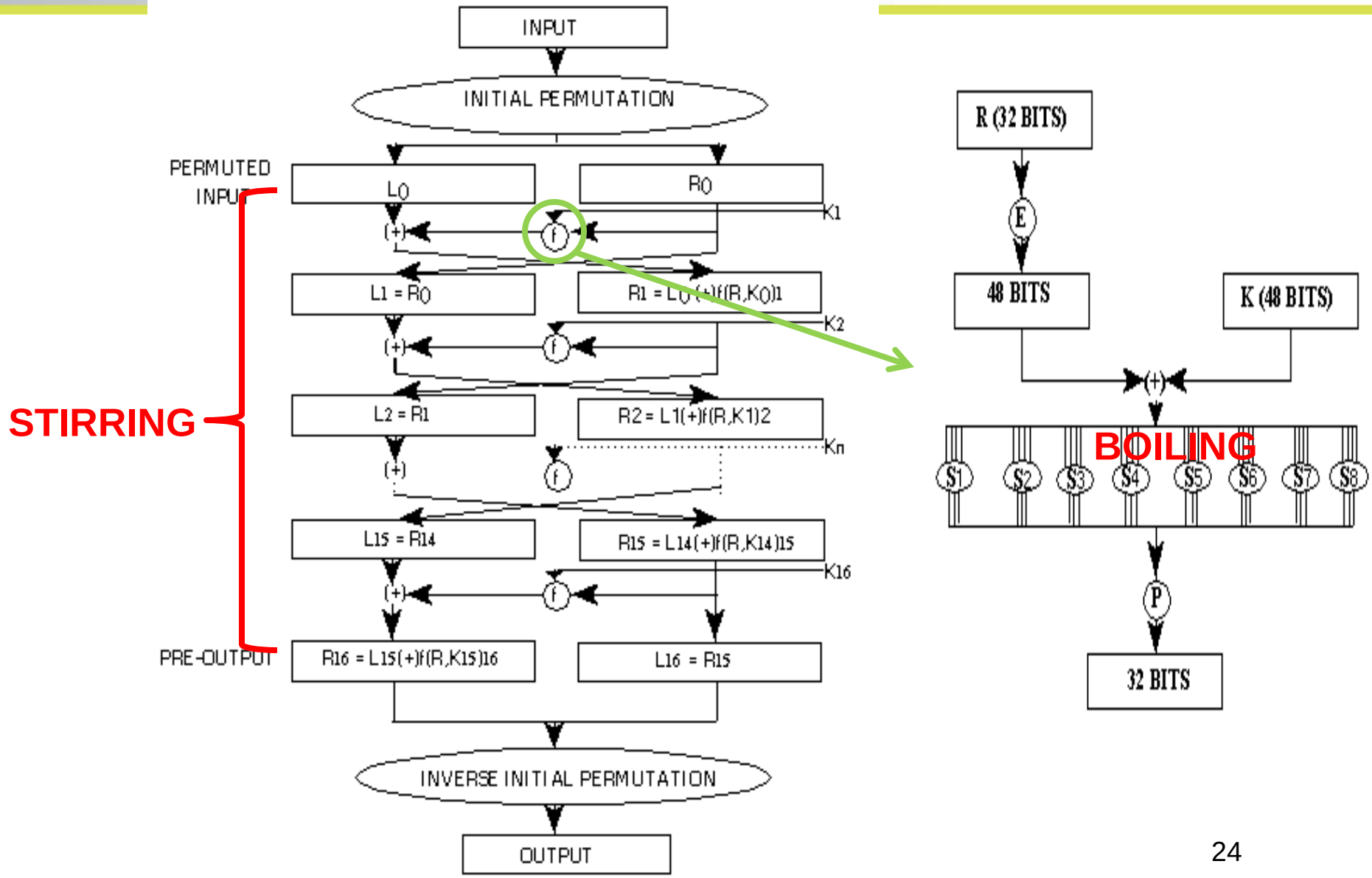
CLASSICAL CRYPTOGRAPHY = Stirring and Boiling!

Stirring = transpositions (re-arrangements)

Boiling = mathematical functions (non-linear)

Alternate Stirring and Boiling (**rounds**)

Data Encryption Standard (1976)



Advanced Encryption Standard (AES)

Education SNIA

National Institute Standards and Technology (NIST)

Competition for DES Replacement

WINNER (2001)

Rijndael

Joan Daemen
Proton World
Belgium

Vincent Rijmen
COSIC
Belgium

What makes Rijndael stand out?

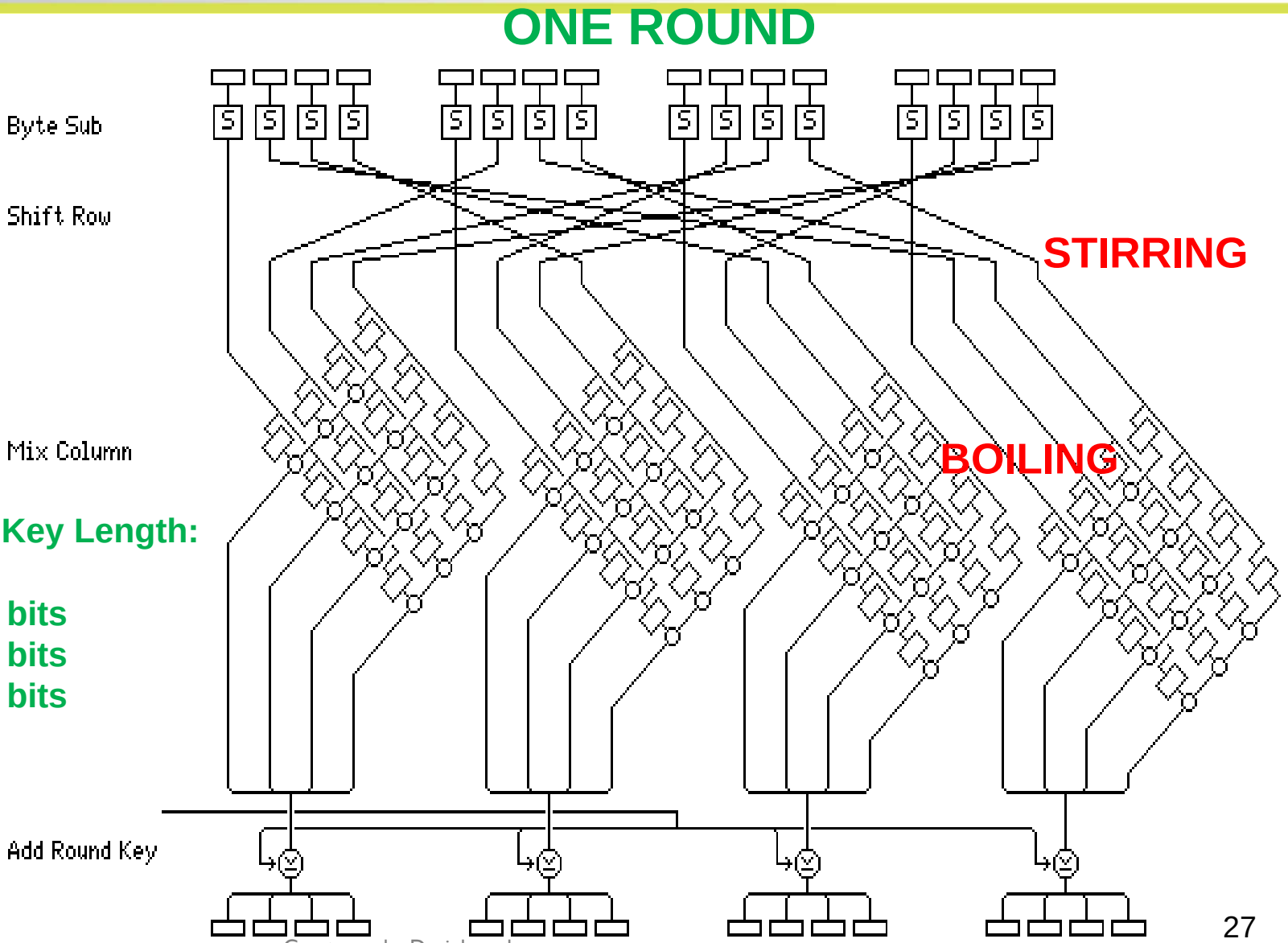
- The symmetric and parallel structure
  - gives implementers a lot of flexibility
  - has not allowed effective cryptanalytic attacks
- Well adapted to modern processors
  - Pentium…
  - RISC and parallel processors
- Suited for Smart Cards (small form factor)
- Flexible in dedicated hardware

→ **Let's have a look at what's inside!**

SNIA Tutorial:

ABCs of Encryption

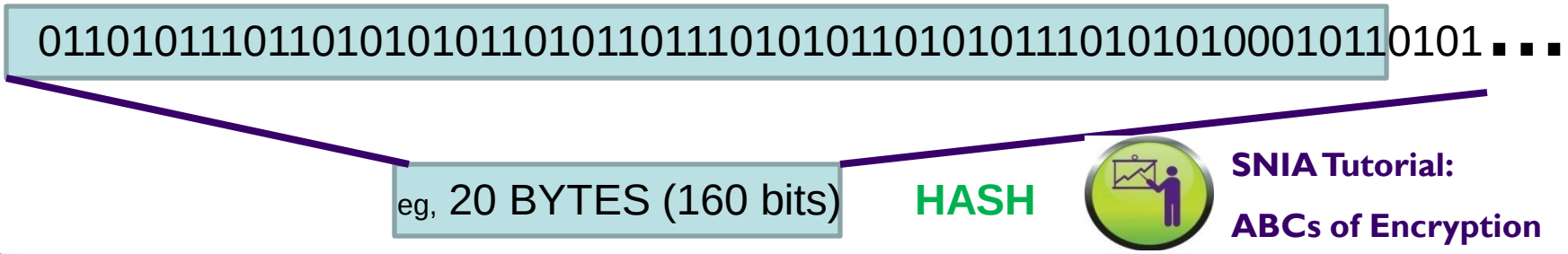
AES (Rijndael) in Hardware



Rounds and Key Length:

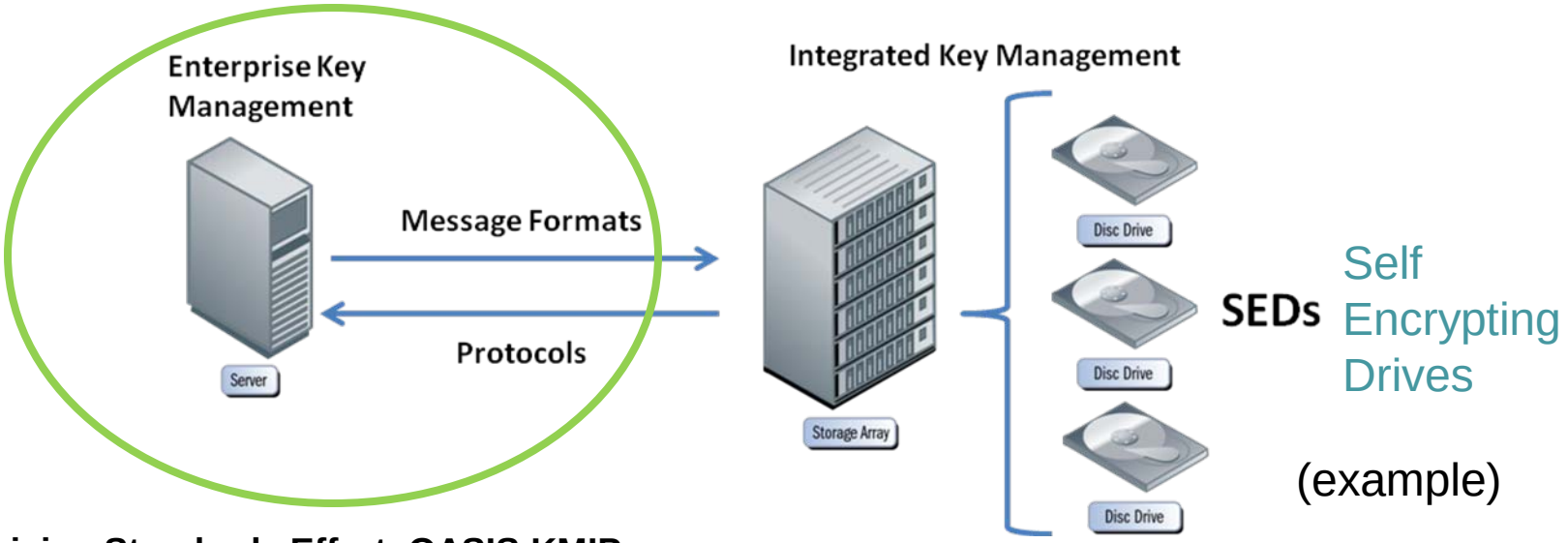
- **10: 128 bits**
- **12: 192 bits**
- **14: 256 bits**

Hashing



- Hashing does not encrypt data, but provides transformation used to verify data integrity
  - Hash algorithm "digests" data into fixed-size equivalent - **HASH**
    - Size of the HASH is fixed by the algorithm (SHA-1 is 20 bytes)
    - Algorithm is non-reversible: cannot reproduce data from hash
    - Single bit change in data may change half of the bits in hash
- Does not require the use of keys
  - But related construct called Message Authentication Code (MAC) uses a hash derived from both data & a secret key
    - HMAC is the best known – see IETF RFC 2104, FIPS PUB 198
- A hash may also be used in a "digital signature" scheme

Key Management

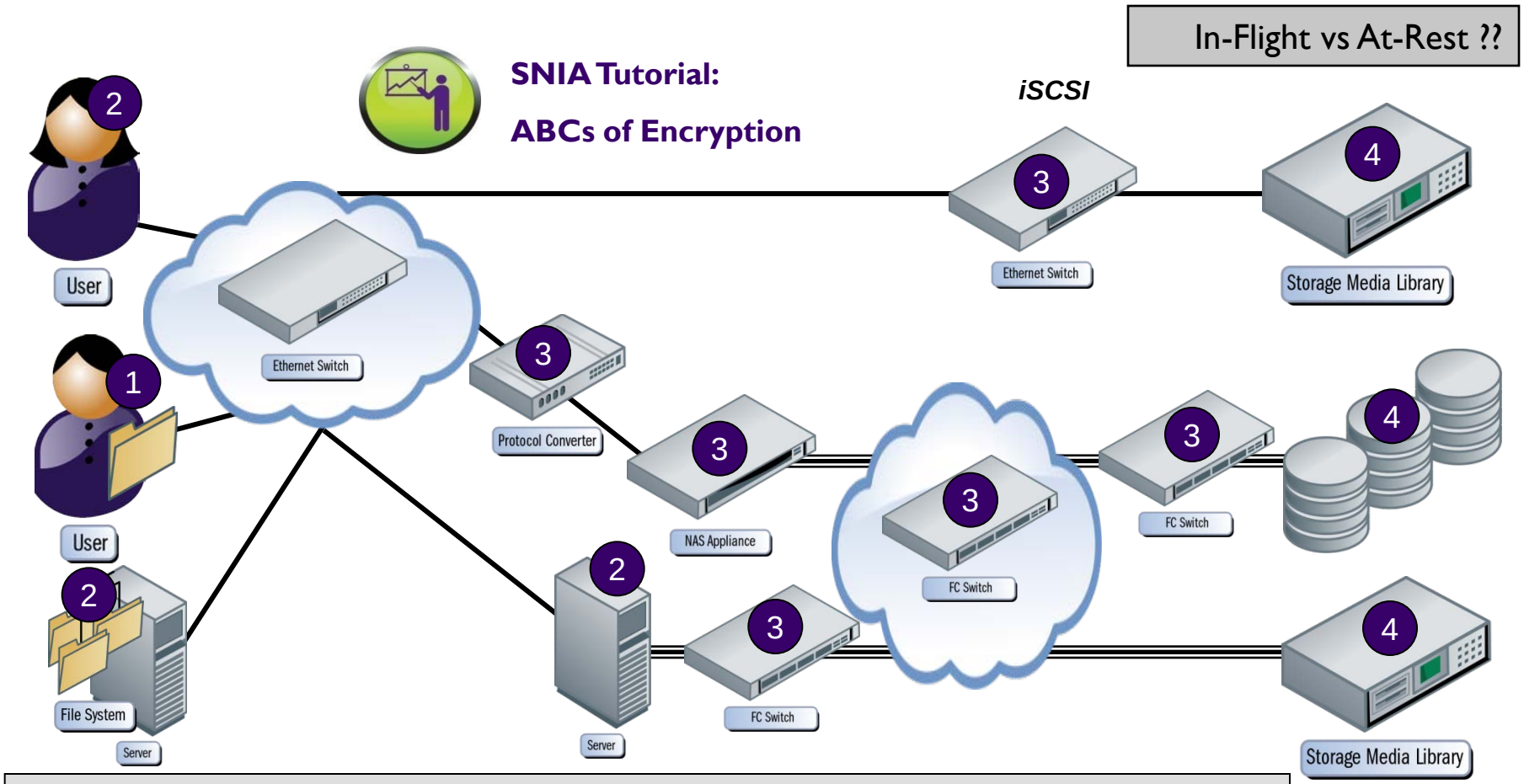


Promising Standards Effort: OASIS KMIP
Key Management Interoperability Protocol
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

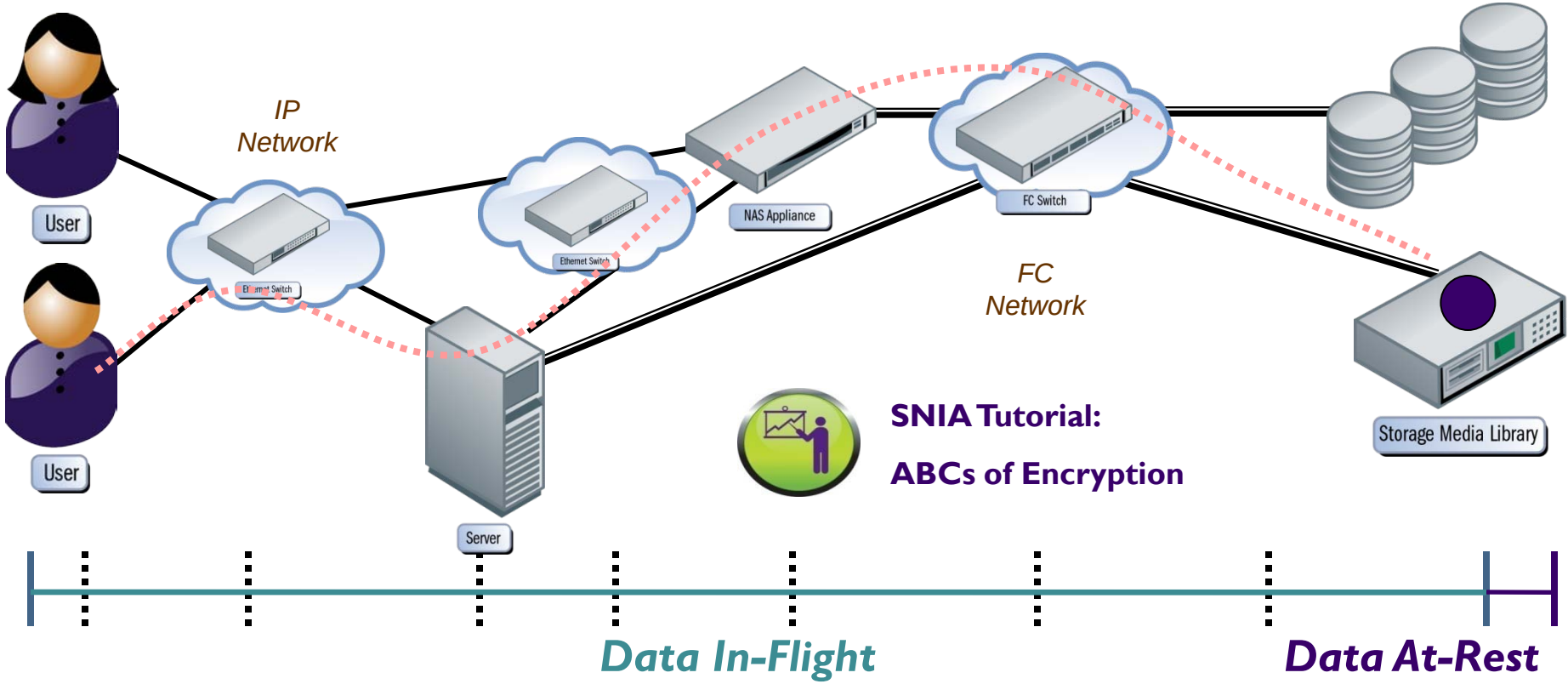
key management: generation, exchange, storage, safeguarding, use, vetting, replacement and finally, destruction of a key.

"Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system." — **Bruce Schneier**, Preface to *Applied Cryptography*, Second Edition.

Points of Encryption



In-Flight versus At-Rest

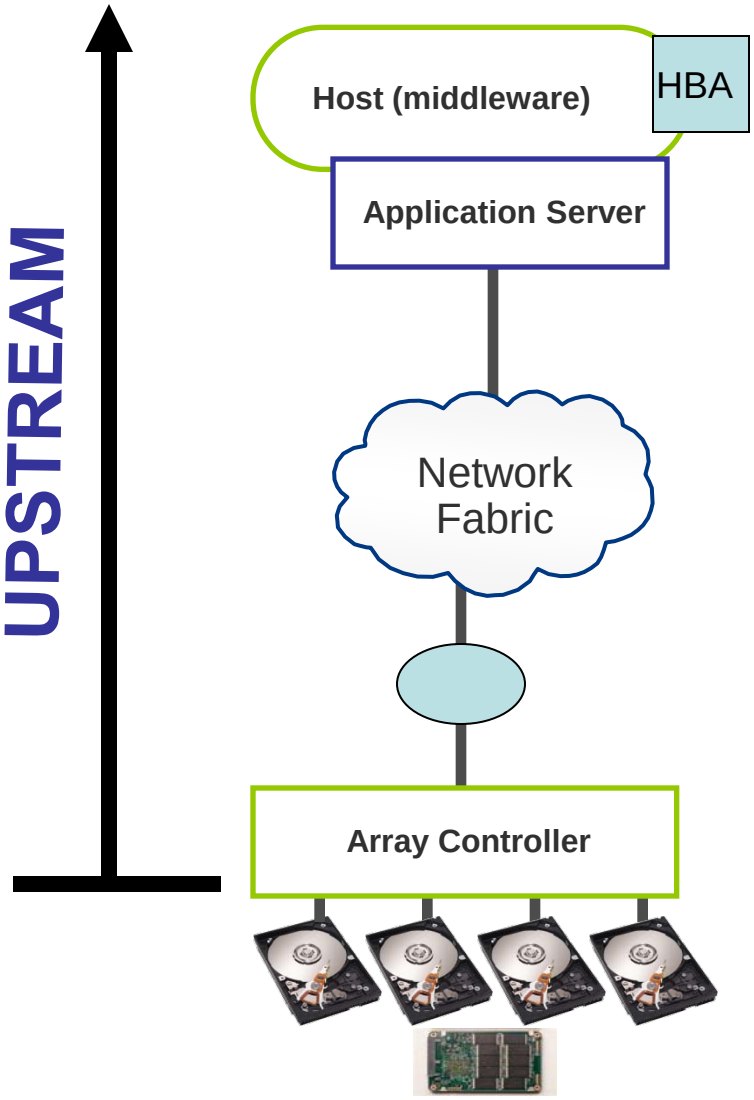


In-Flight:
- Two end points (communication)
- Interoperability – network layers
- Data is transitory (temporary)

At-Rest:
- Interoperability – media interchangeability
- Data is persistent on media
  - Plaintext to L, Ciphertext to R

Yes, the term is a misnomer because media moves!

Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

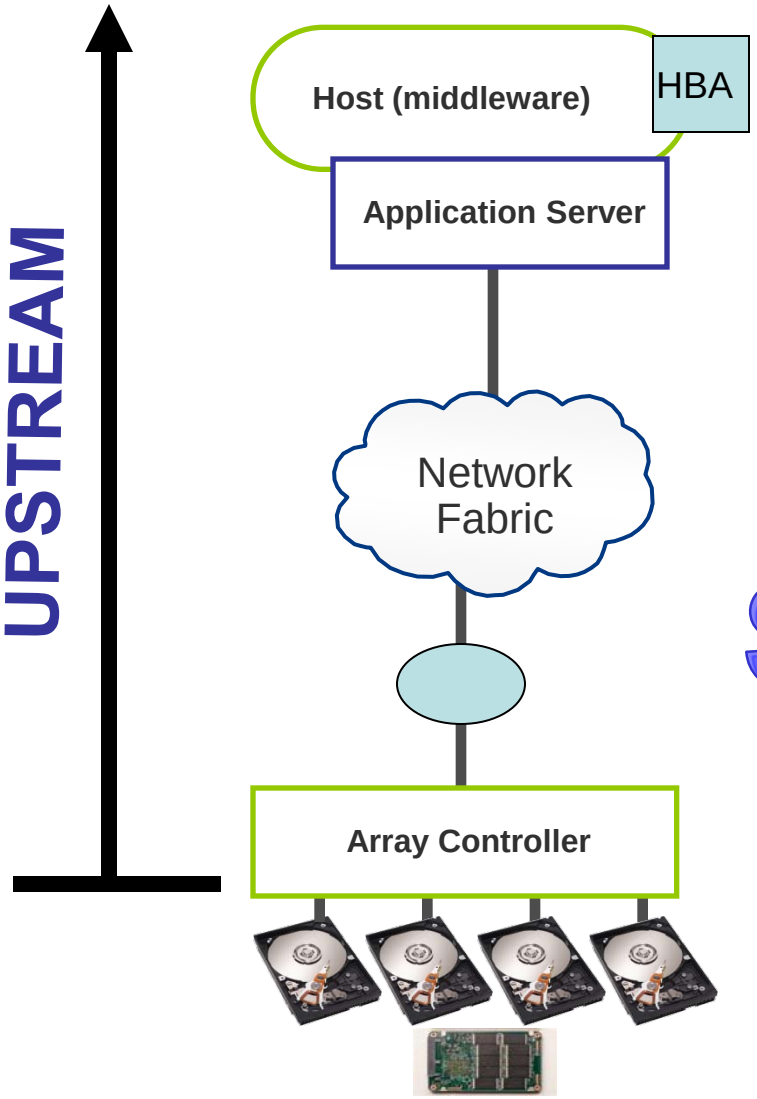
Switch

"Bump in the wire" appliance

Array controller

Drive (HDD, SSD)

Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

Switch

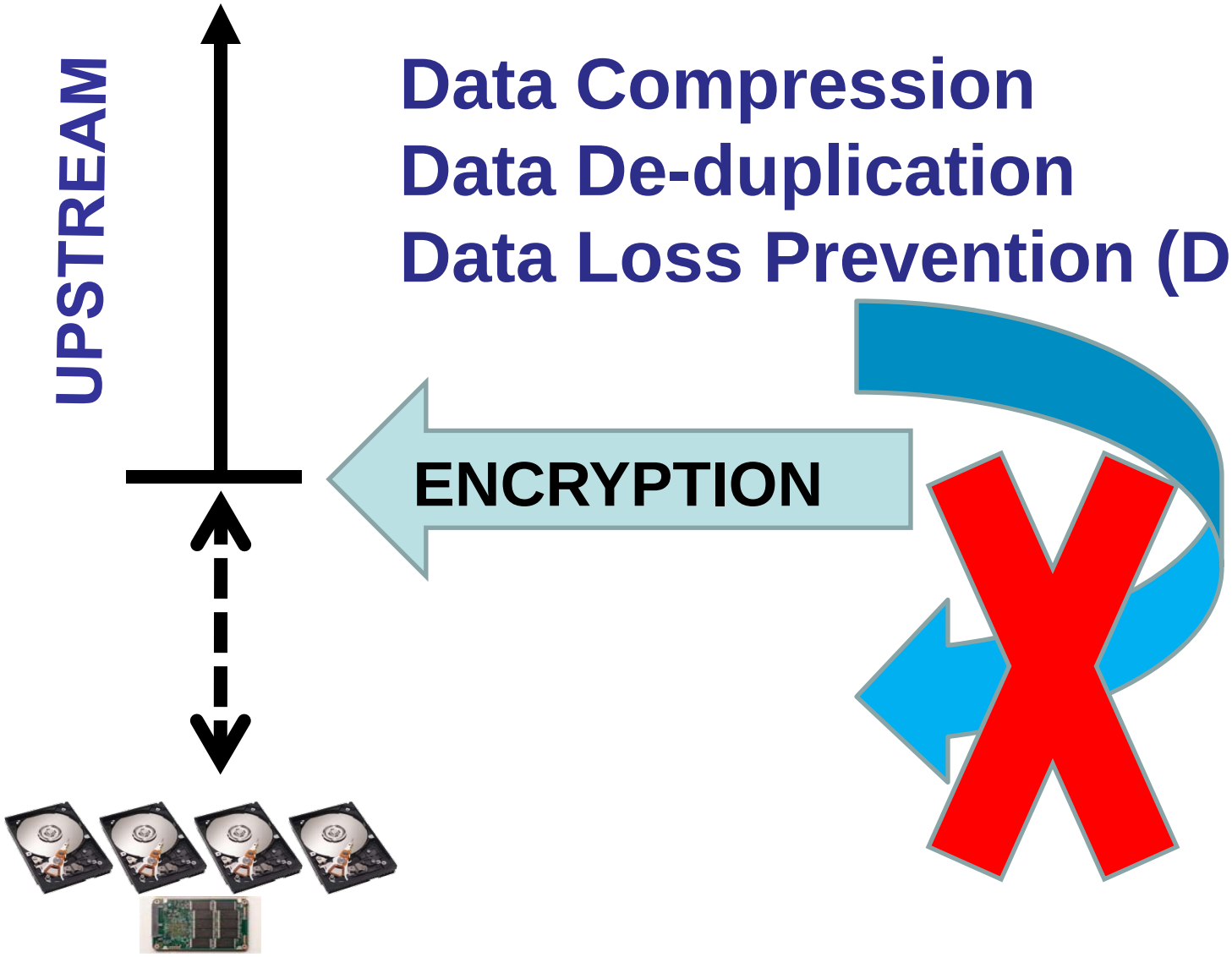
"Bump in the wire" appliance

Array controller

Drive (HDD, SSD)

DIFFERENT THREAT SCENARIOS

Encryption upstream can affect other processes



Why Encrypt Data-At-Rest?

Education SNIA

- Compliance
  - **46+ states have data privacy laws with encryption "safe harbors", which exempt encrypted data from breach notification[1]**

- Data center and laptop drives are portable (HDD, SSD)
- Exposure of data loss is expensive ($6.65 Million on average per incident[2])
- Obsolete, Failed, Stolen, Misplaced…
  - **Nearly ALL drives leave the security of the data center**
  - **The vast majority of decommissioned drives are still readable**

Threat scenario: stored data leaves the owner's control – lost, stolen, re-purposed, repaired, end-of-life, …

1. http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx
2. Ponemon Institute, Fourth Annual US Cost of Data Breach Study – Jan 2009 www.ponemon.org

Built-In Data At-Rest Encryption

- Encryption/decryption built into tape drives
  - Encryption AFTER compression (to keep usual ratio)
  - Key not stored on the media or retrievable from drive
    - Key-associated data to help in "found tape" case
  - Tape-to-tape copy without decryption being worked
- Encryption/decryption built into disk drives
  - Data encrypted before storing on media, decrypted when read
  - Can be "crypto erased" by replacing the on-board key
    - But will wipe all existing data; start over with a clean drive
  - Defined by Trusted Computing Group (TCG)
- Encryption/decryption built into SSD or Flash drives

SNIA Tutorial:

ABCs of Encryption

Check out SNIA Tutorial:

Self-Encrypting Drives

Data In-Flight Encryption

- Technology differs by "transport"
  - Block-level IP protocols
    - IPsec for iSCSI, iFCP, FCIP
  - Block-level, FC protocols
    - FC-SP, ESP_Header, CT protection
  - File-level, IP protocols
    - IPsec for NFS & SMB/CIFS
    - SSL/TLS for WebDAV
  - Management protocols
    - SSL/TLS or SSH for SMI-S, SNMPv3, web-based mgmt
- IPsec & TLS largely proven
  - Widely deployed for VPNs, less so for traffic inside the corporate firewall
- SCSI Command Sets now also incorporate protection mechanisms (e.g. ESP-SCSI)
- There may be others…

SNIA Tutorial:

ABCs of Encryption

Both In-Flight & At-Rest

- Host Bus Adapter- & Array Controller-based encryption
- Security appliances & switch-based encryption
  - Most also compress data before encryption (to keep historical efficiencies)
  - Also include key management functions
- Applications with encryption features
  - Many have been around for quite a while!
- New OS offerings & encrypting file systems
- New NAS & CIFS products will emphasize security
  - Some have purpose-designed cryptographic schemes
- Remember – all encryption points have to be authenticated & provisioned with keys

SNIA Tutorial:

ABCs of Encryption

Summary

- New storage products with data-at-rest encryption are becoming available that address major users' concerns
  - Based on industry standards, utilizing new features in SCSI and ATA interfaces and command sets
- Nine-Step Checklist defines the tasks you need to complete to best utilize data-at-rest encryption products in your organization
- Also see: Security Best Current Practices (SNIA/SSIF)

SNIA Tutorial:

ABCs of Encryption

Core and technology-specific BCPs:

- **Core:**
  - General Storage Security
  - Storage Systems Security
  - Storage Management Security
- **Technology-specific:**
  - Network Attached Storage (NAS)
  - Block-based IP Storage
  - Fibre Channel Storage
  - **Encryption for Storage**
  - Key Management for Storage
  - Long-term Information Security

http://www.snia.org/forums/ssif/programs/SNIATechnicalProposal-Security-BCPs.20080904.pdf

SNIA Nine-Step Checklist

Education SNIA

"Encryption of Data at Rest – a Step by Step Checklist"

(revised Sept/2009)

(available @ http://www.snia.org/forums/ssif/knowledge_center/white_papers/)

SNIA Tutorial:

ABCs of Encryption

Introduction

- Step-by-step listing of tasks to be performed to effectively implement **at-rest** data encryption
  - Defines a process, not a single activity
  - Not all sub-steps will be needed in all cases, but they all merit consideration
- SNIA/SSIF checklist document contains annexes with useful additional checklists related to security & encryption from:
  - Federal Financial Institutions Examination Council (FFIEC)
  - Information Systems Audit and Control Association (ISACA)
  - Payment Card Industry (PCI) Data Security Standard (DSS)

SNIA Tutorial:

ABCs of Encryption

The Steps

1. Understand Drivers
2. Classify Data Assets
3. Inventory Data Assets
4. Perform Data Flow Analysis
5. Choose Points-of-Encryption
6. Design Encryption Solution
7. Begin Data Re-Alignment
8. Implement Solution
9. Activate Encryption

SNIA Tutorial:

ABCs of Encryption

So you're done, right?

- Still need to perform regular point tests
  - Don't rely on users to detect problems for you
- Regularly audit the logs to ensure all relevant information being captured
  - When the external auditors are coming next week, it's too late to find out that info hasn't been captured

SNIA Tutorial:

ABCs of Encryption

Summary

- A number of secure storage products are now available
  - Based on industry standards!
- Addressing major concerns by use of storage security becomes feasible for the first time
- Encryption within a SAN or a storage device is only one part of a total solution
  - You'll need multiple "layers" for fully effective protection; i.e., defense in depth
  - You'll need a wider scope than just storage security to satisfy regulatory obligations (e.g. PCI DSS)
- This tutorial has:
  - Defined the terminology
  - Introduced the underlying protocols & approaches
  - Laid out a process to follow when fielding storage security products

SNIA Tutorial:

ABCs of Encryption

Get Involved… !!

SNIA Security

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups
- Storage Security Industry Forum (SSIF)
  - Focus: Marketing collateral, educational materials, customer needs, whitepapers including the BCPs & Encryption of Data At-Rest (a Step-by-Step Checklist)
  - http://www.snia.org/forums/ssif

SNIA Tutorial:

ABCs of Encryption

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Roger Cummings!!

Eric A. Hibbard, CISSP, CISA
SNIA SSIF
Gianna DaGiau

Storage Security Standards Orgs

- ISO/IEC JTC1 SC27 – IT Security Techniques (www.iso.org/iso/iso_technical_committee?commid=45306)
  - US group is ANSI/INCITS CS1 (cs1.incits.org)
- NIST/CSD Computer Security Resource Center (csrc.nist.gov) – Security standards for US Government
- IEEE/P1619 (siswg.net) – Security in Storage Working Group
- ANSI/INCITS T10 (www.t10.org) – SCSI security, tape drive encryption control
- ANSI/INCITS T11 (www.t11.org) – Fibre Channel security (FC-SP)
- ANSI/INCITS T13 (www.t13.org) – (S, P)ATA
- IETF (www.ietf.org) – IP security (IPsec), Transport Layer Security (TLS)
- TCG (www.trustedcomputinggroup.org) – self-encrypting storage

Web Sources of Information

- The CERT® Coordination Center, http://www.cert.org
- The SANS (SysAdmin, Audit, Network, Security) Institute, http://www.sans.org
- The Center for Internet Security (CIS), http://www.cisecurity.org
- Information Systems Audit and Control Association (ISACA) – *IS Standards, Guidelines, and Procedures for Auditing and Control Professionals*, http://www.isaca.org/standards/
- Information Security Forum (ISF) – The Standard of Good Practice for Information Security, http://www.isfsecuritystandard.com/

SNIA Tutorial:

ABCs of Encryption

REFERENCES

- Handbook of Applied Cryptography, Menezes/VanOorschot/Vanstone, CRC Press, NY, 1997.

- Applied Cryptography, Bruce Schneier, Wiley and Sons, NY, 1996 (second edition).

- http://theory.lcs.mit.edu/~rivest/

- (historical) The Codebreakers, David Kahn, Macmillan, NY, 1967.