An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 7

Required Week Seven Readings

1. "THE POSSIBILITY OF SECURE NON-SECRET DIGITAL ENCRYPTION
by J. H. Ellis, January 1970
https://cryptocellar.org/cesg/possnse.pdf

***2.* Finish Reading "*From CIA to APT: An Introduction*"**
***to Cyber Security*, E. Amoroso & M. Amoroso**

LinkedIn: Edward Amoroso

How Does Conventional Cryptography Work?

Definition: Cryptosystem

A cryptosystem is a five-tuple consisting of

- Encryption function E
- Decryption function D
- Set of plaintext elements P
- Set of ciphertext elements C
- Set of cryptographic keys K

Week 7

Definition: Cryptosystem

A cryptosystem is a five-tuple consisting of

- Encryption function E
- Decryption function D
- Set of plaintext elements P
- Set of ciphertext elements C
- Set of cryptographic keys K

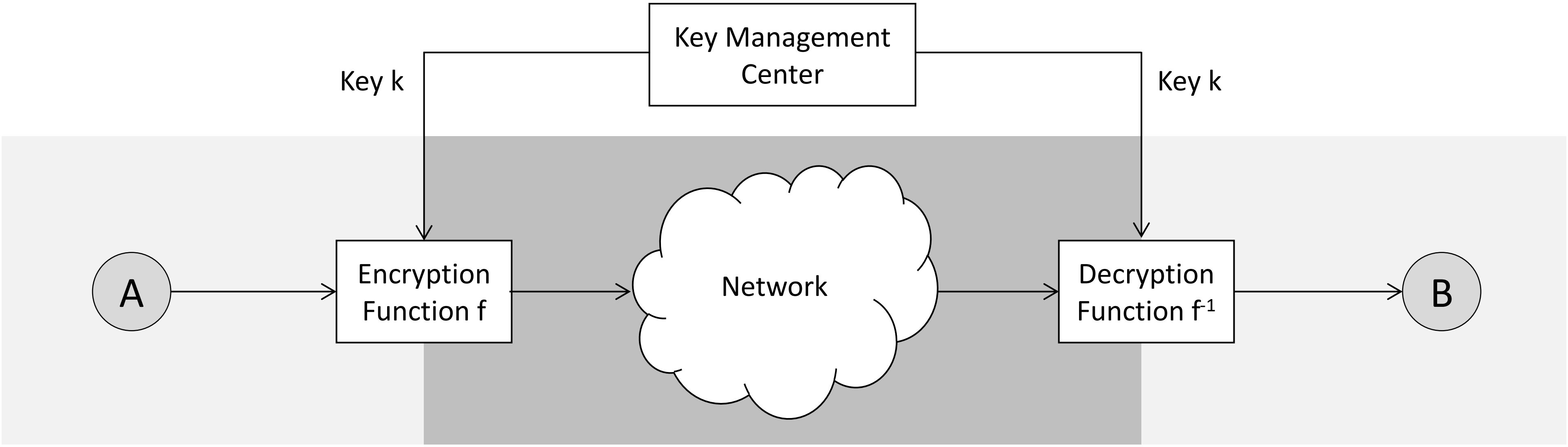
$E(p) = c$	$\{ p \} = c$
$D(c) = p$	$\{ c \} = p$
$D (E (p))$	$\{ \{ p \} \} = p$
$E_k(p) = c$	$\{ p \}_k = c$
$D_k(c) = p$	$\{ \{ p \}_k \}_k = p$

Encrypt

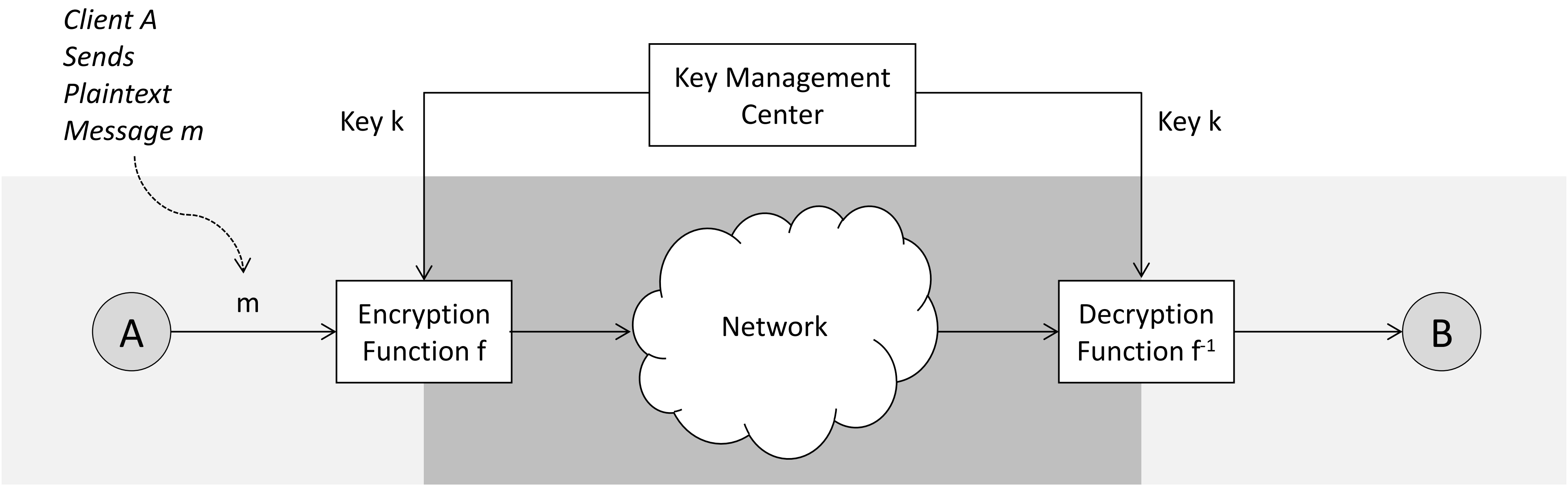
Decrypt

Week 7

Conventional Encryption Schema

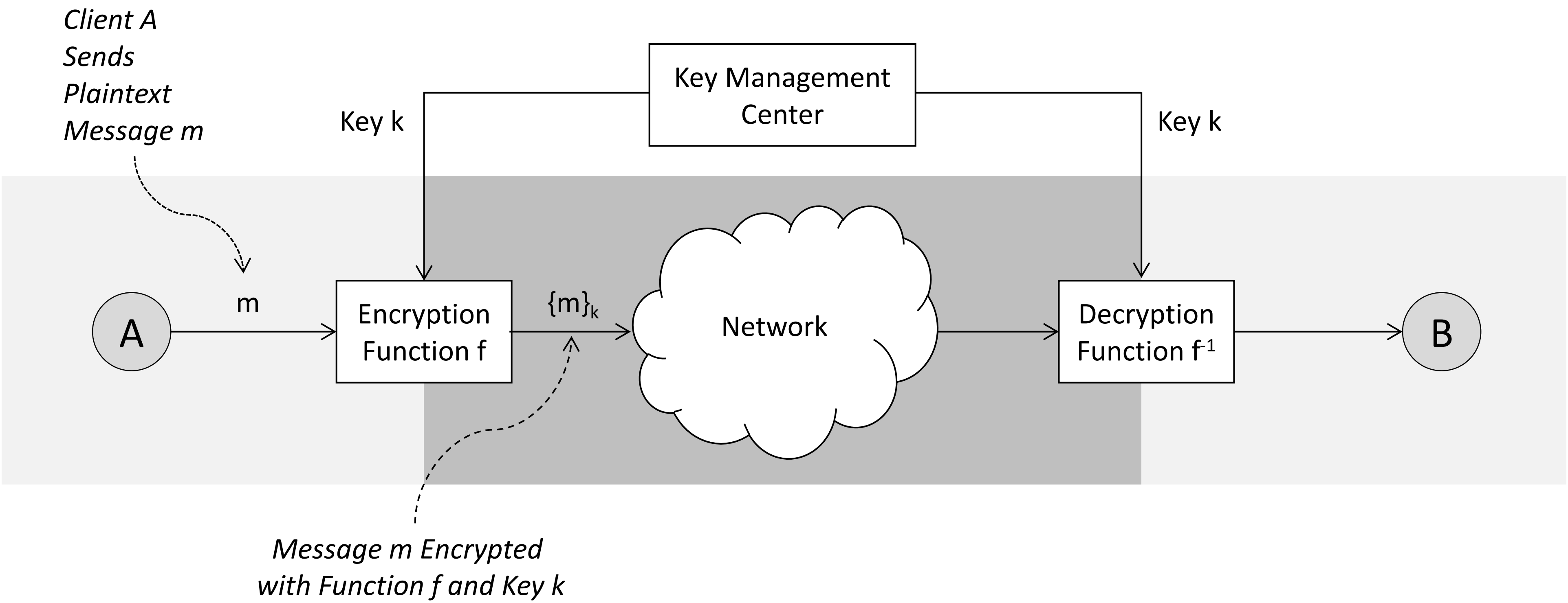


Conventional Encryption Schema



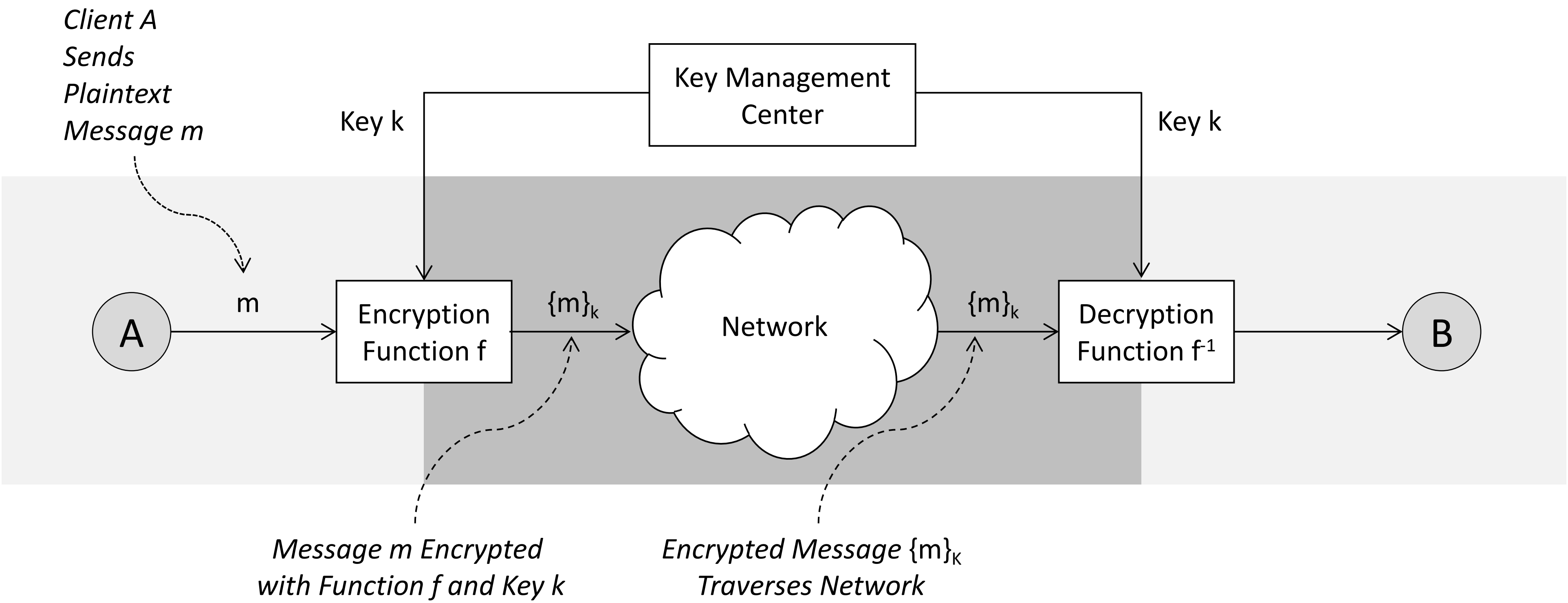
Week 7

Conventional Encryption Schema

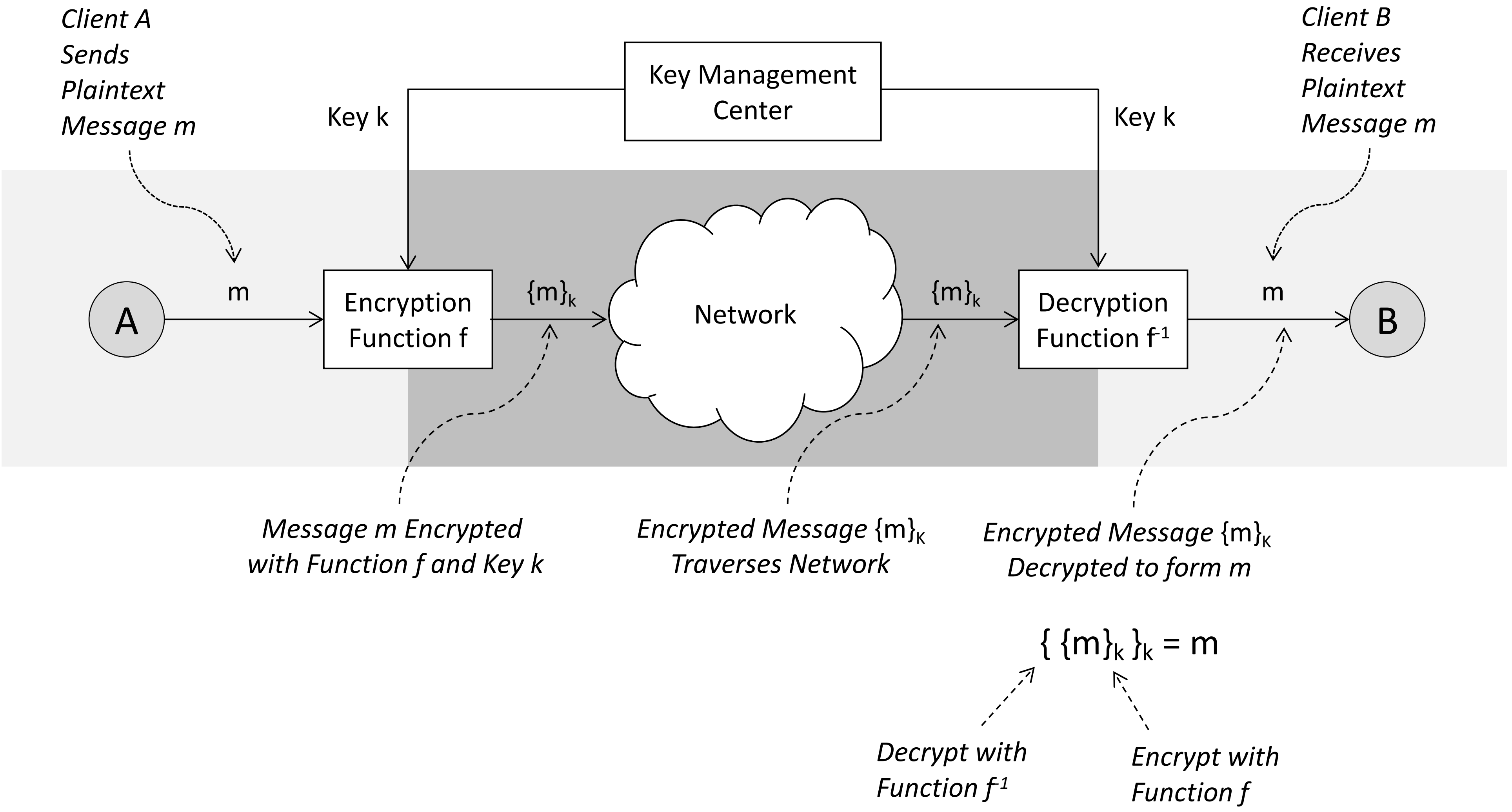


Week 7

Conventional Encryption Schema

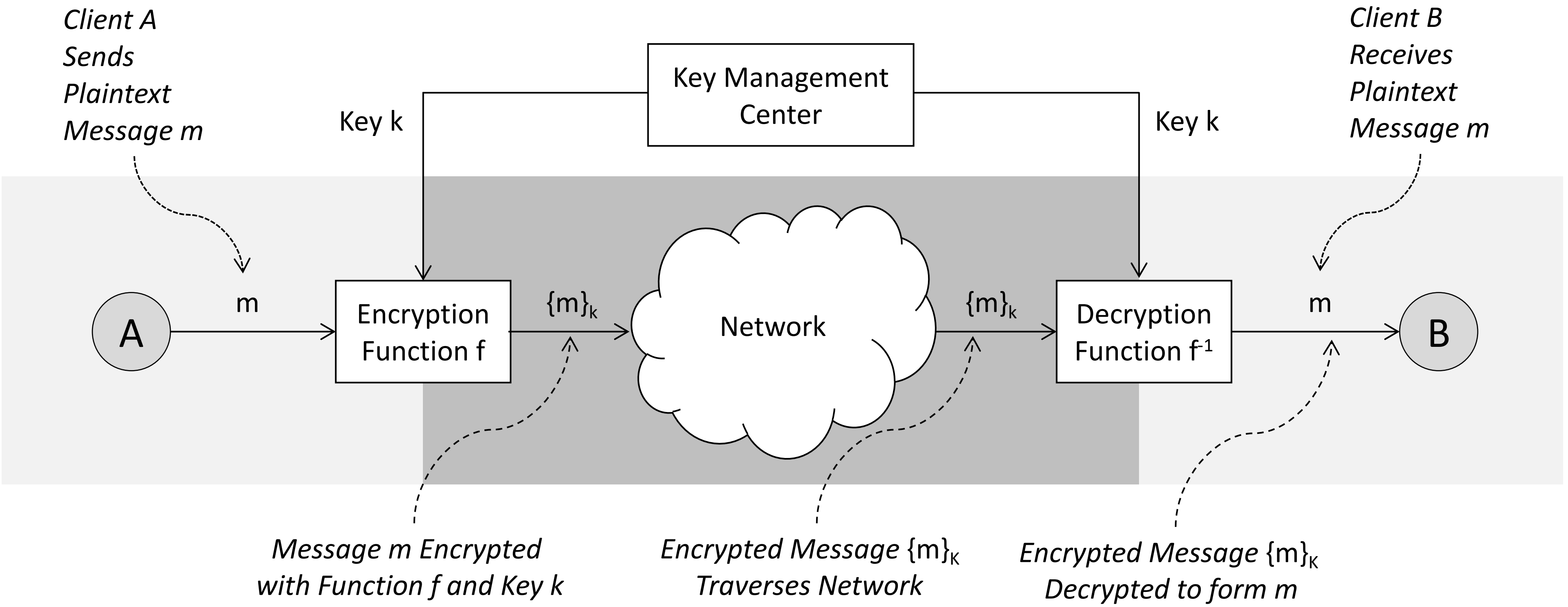


Conventional Encryption Schema



Week 7

Conventional Encryption Schema



$$\{\ \{m\}_k\ \}_k = m$$

Decrypt with Function f^{-1}

Encrypt with Function f

Two Important Security Properties:

1. Secrecy Between A and B
2. Authentication of A by B

What is the Simplest Example Encryption Algorithm?

Week 7

XOR Function

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

Week 7

XOR Function

`Plaintext Input      0 0 1 0  0 0 1 1`

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

XOR Function

```
Plaintext Input      0 0 1 0  0 0 1 1

Key                  1 1 1 0  1 1 1 0
```

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

Week 7

XOR Function

Plaintext Input	0 0 1 0 0 0 1 1
Key	1 1 1 0 1 1 1 0
Ciphertext	1 1 0 0 1 1 0 1

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

Week 7

XOR Function

Plaintext Input	0 0 1 0 0 0 1 1
Key	1 1 1 0 1 1 1 0
Ciphertext	1 1 0 0 1 1 0 1
Key	1 1 1 0 1 1 1 0

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

XOR Function

Plaintext Input	0 0 1 0	0 0 1 1
Key	1 1 1 0	1 1 1 0
Ciphertext	1 1 0 0	1 1 0 1
Key	1 1 1 0	1 1 1 0
Plaintext Output	0 0 1 0	0 0 1 1

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

Conventional Encryption Algorithm – Simplest Example

What are the Two Most Basic Design Strategies for Encryption Algorithms?

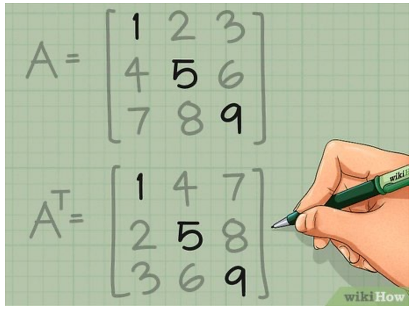
Substitution Cipher – Replacement of one or more things with one or more things (Symmetric versus Asymmetric)

Conventional Encryption Algorithm – Strategies

Week 7

Substitution Cipher – Replacement of one or more things with one or more things (Symmetric versus Asymmetric)

Transposition Cipher – Use of matrix arithmetic to represent and manipulate text (Linear Algebraic basis)



Conventional Encryption Algorithm – Strategies

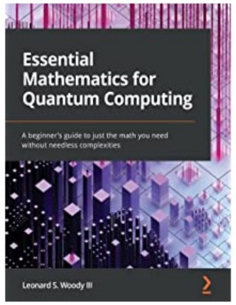
Week 7

All | Same-Day Delivery | Customer Service | Amazon Basics | Home Improvement | Groceries | Amazon Home | Beauty & Personal Care | Health & Household

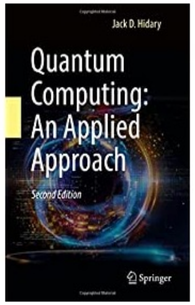
Advanced Search | New Releases | Best Sellers & More | Amazon Book Clubs | Children's Books | Textbooks | Textbook Rentals | Best Books of the Month

Customers who viewed this item also viewed

Quantum Algorithms via Linear Algebra: A Primer (The MIT Press)
15
$45.00 prime



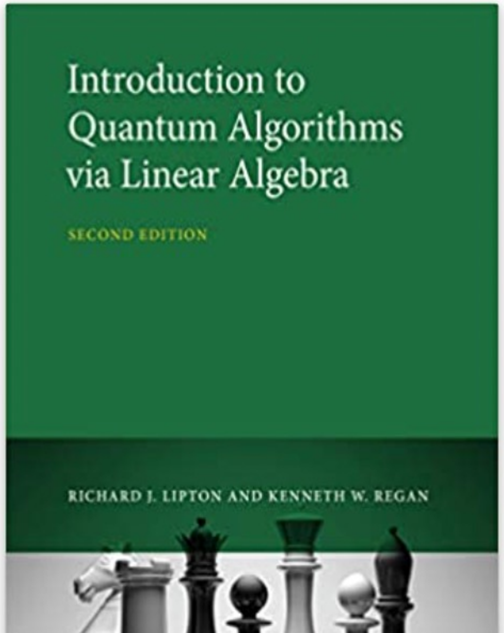
Essential Mathematics for Quantum Computing: A beginner's guide to just the math you need without needless complexities
28
$46.99 prime



Quantum Con
$26.49 prim

Books › Computers & Technology › Computer Science

Look inside



Introduction to Quantum Algorithms via Linear Algebra, second edition 2nd Edition

by Richard J. Lipton (Author), Kenneth W. Regan (Author)

5 ratings

See all formats and editions

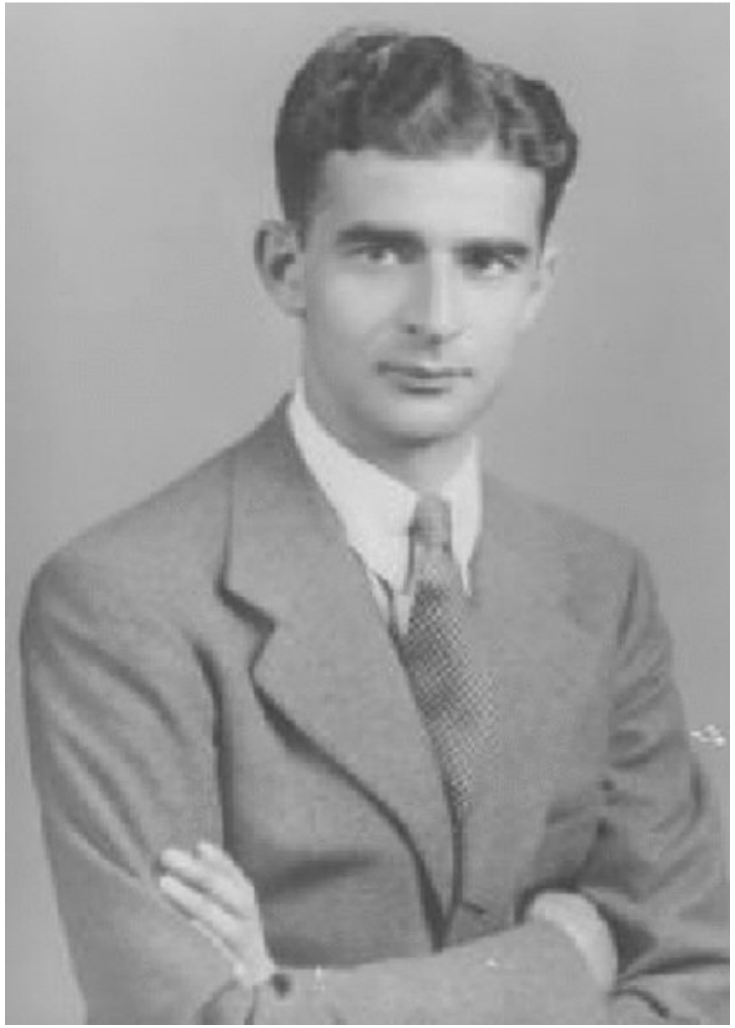
Kindle	Hardcover
$27.99	$34.27 - $45.00 prime
Read with Our Free App	8 Used from $34.27 20 New from $39.15

Buy
prii
FREE
FREE
22. C
De
07
Only
way)
Qty:

Quantum computing explained in terms of elementary linear algebra, emphasizing computation and algorithms and

What is the Data Encryption Standard (DES)?
(How Did It Influence AES?)

Week 7



United States Patent [19]

Feistel

[11] **3,798,359**

[45] **Mar. 19, 1974**

[54] **BLOCK CIPHER CRYPTOGRAPHIC SYSTEM**

[75] Inventor: **Horst Feistel,** Mount Kisco, N.Y.

[73] Assignee: **International Business Machines Corporation,** Armonk, N.Y.

[22] Filed: **June 30, 1971**

[21] Appl. No.: **158,360**

[52] **U.S. Cl.** **178/22,** 340/172.5, 340/348

[51] **Int. Cl.** **H04l 9/00**

[58] **Field of Search** 178/22; 340/172.5, 348

[56] **References Cited**

UNITED STATES PATENTS

3,657,699	4/1972	Rocher	178/22
2,984,700	5/1961	Small	178/22
3,170,033	2/1965	Vasseur	178/22
2,995,624	8/1961	Watters	178/22
2,917,579	12/1959	Hagelin	178/22

Primary Examiner—Benjamin A. Borchelt
Assistant Examiner—H. A. Birmiel
Attorney, Agent, or Firm—Victor Siber

[57] **ABSTRACT**

nary data under the control of a key consisting of a set of binary symbols. The cryptographic system is utilized within a data processing environment to ensure complete privacy of data and information that is stored or processed within a computing system. All authorized subscribers who are permitted access to data within the network are assigned a unique key consisting of a combination of binary symbols. The central processing unit within the computing network contains a complete listing of all distributed authorized subscriber keys. All communications transmitted from terminal input are encrypted into a block cipher by use of the cryptographic system operating under the control of the subscriber key which is inputed to the terminal device. At the receiving station or central processing unit, an identical subscriber key which is obtained from internal tables stored within the computing system is used to decipher all received ciphered communications.

The cryptographic system develops a product cipher which is a combination of linear and nonlinear transformations of the clear message, the transformation being a function of the binary values that appear in the subscriber key. In addition to the transformation, the key controls various register substitutions and modulo-2 additions of partially ciphered data within the cryptographic system.

Data Encryption Standard (DES)

64-bit block input

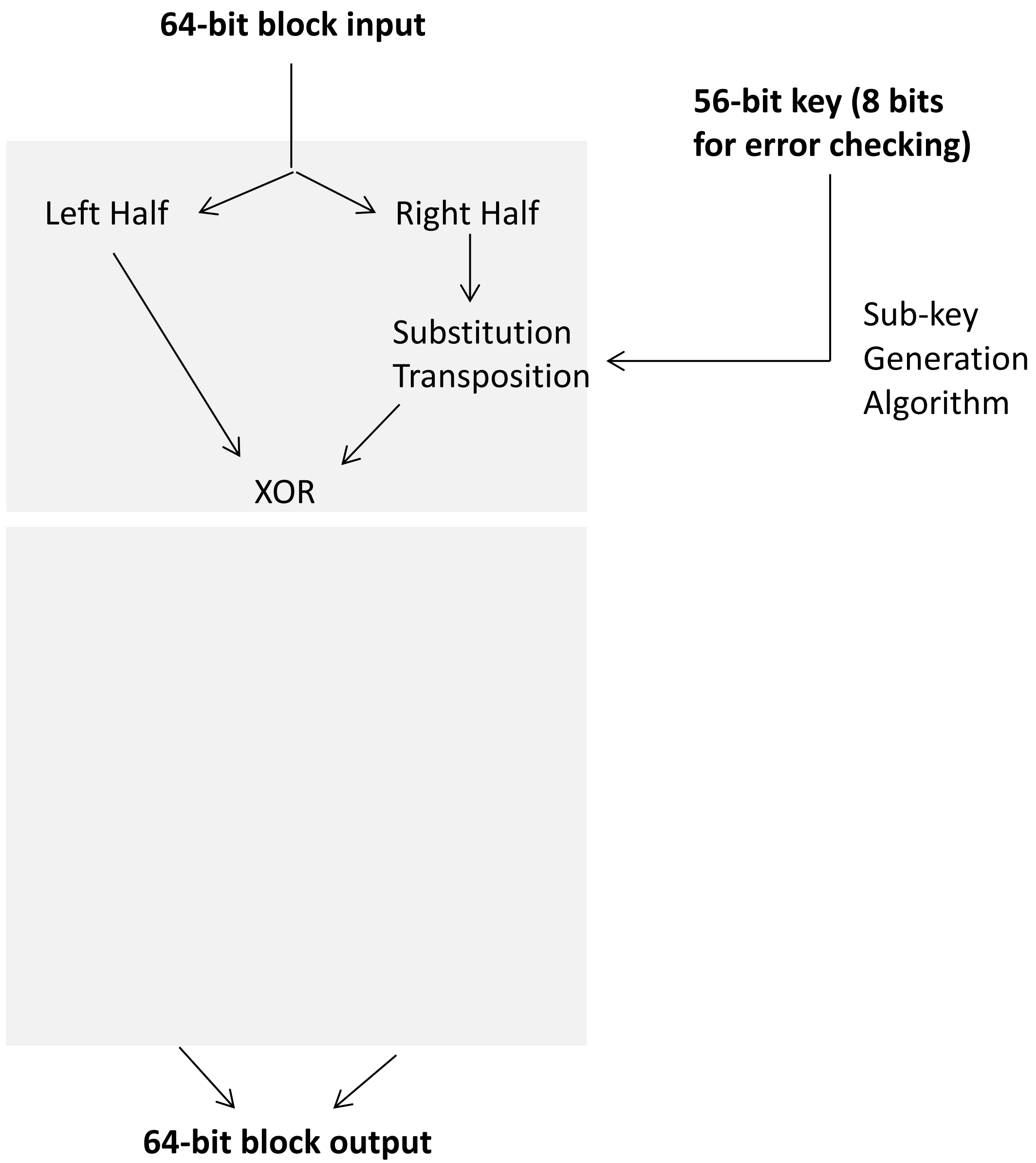
56-bit key (8 bits for error checking)

Original National Bureau of Standards (NBS) in Washington

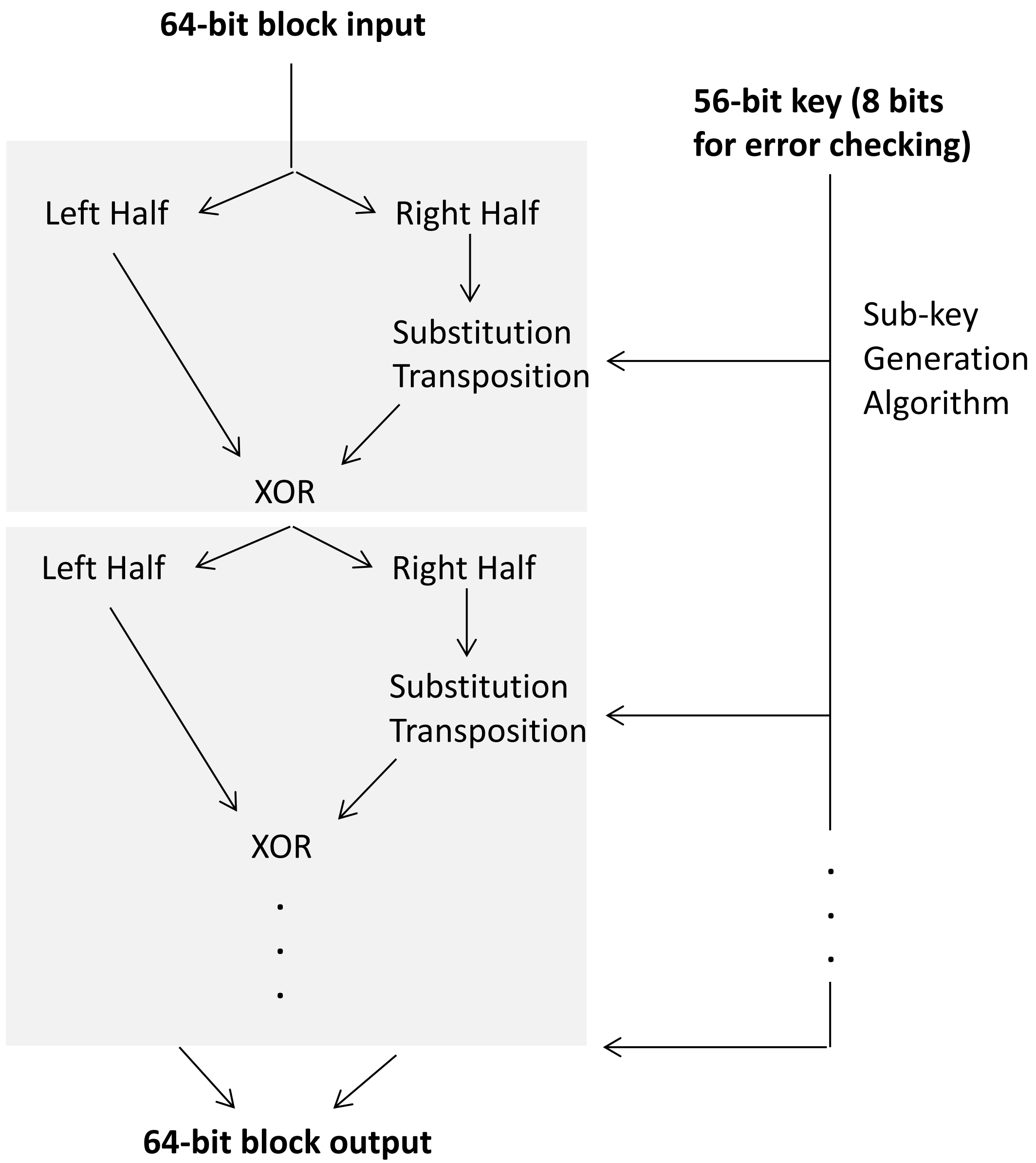
64-bit block output

Week 7

Data Encryption Standard (DES)

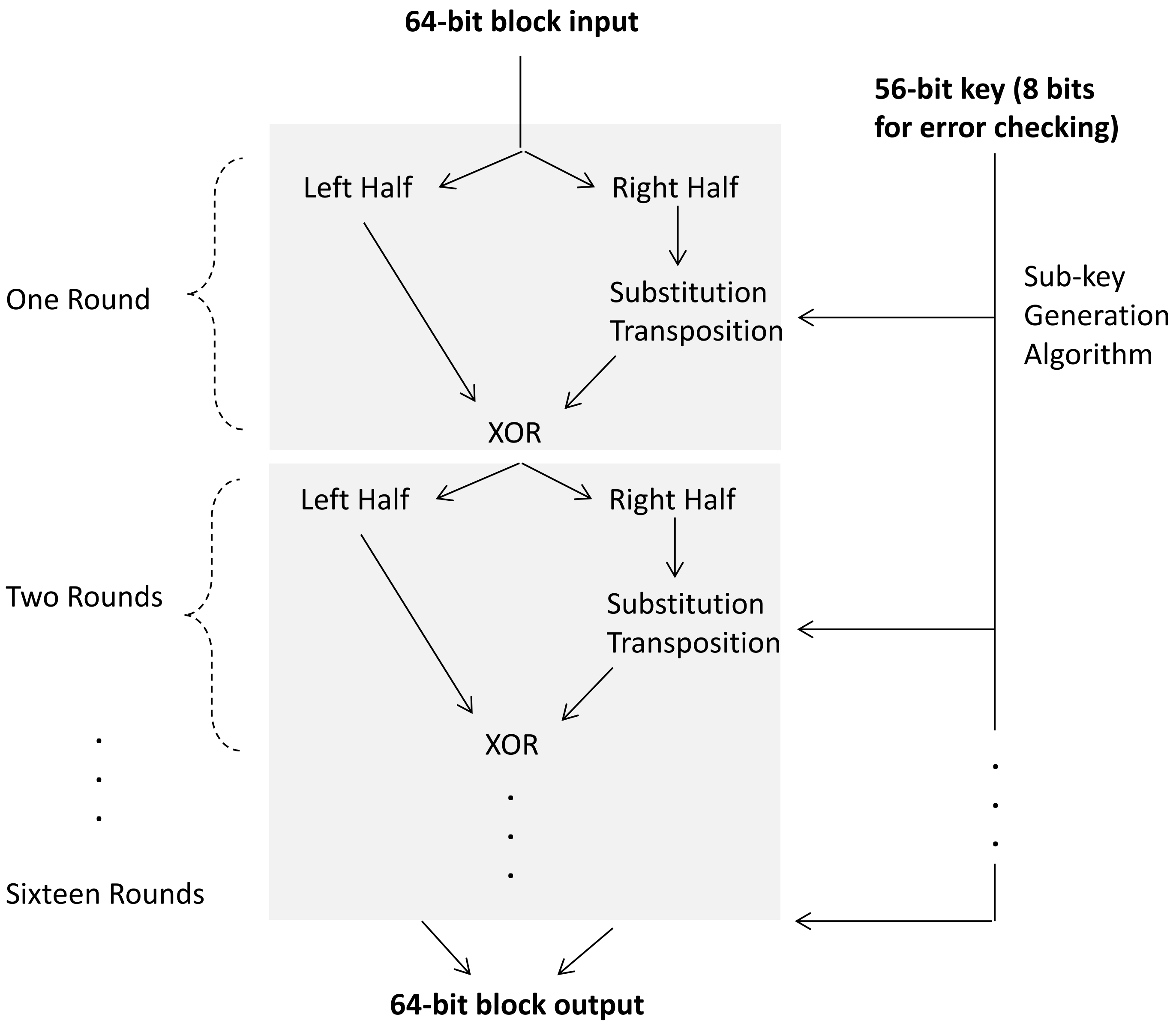


Data Encryption Standard (DES)

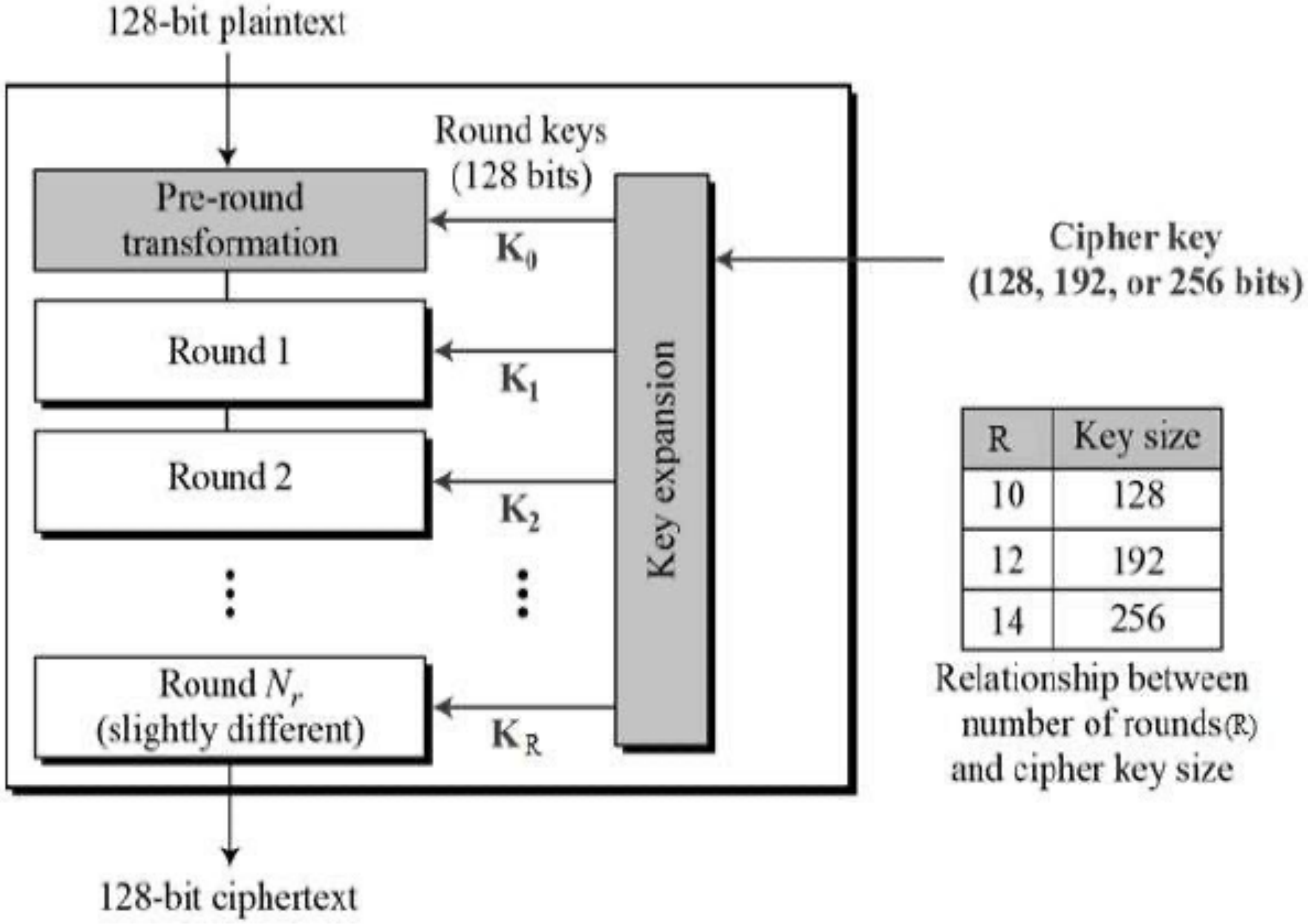


Week 7

Data Encryption Standard (DES)



Advanced Encryption Standard (AES)



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

What is Triple DES (3DES)?
(How Did It Solve Key Length Issues and 1DES Interoperability?)

Week 7

Walt Tuchman – IBM
Circa 1981

Triple-DES

$\{ m \}_{K1}$	Single-DES	56 Bit Key

Triple-DES

$\{ m \}_{K1}$	Single-DES	56 Bit Key
$\{ \{ m \}_{K1} \}_{K2}$	Double-DES	112 Bit Key

Triple-DES

$\{ m \}_{K1}$	Single-DES	56 Bit Key
$\{ \{ m \}_{K1} \}_{K2}$	Double-DES	112 Bit Key
$\{ \{ \{ m \}_{K1} \}_{K2} \}_{K3}$	Triple-DES	168 Bit Key

Triple-DES

$\{ m \}_{K1}$	Single-DES	56 Bit Key
$\{ \{ m \}_{K1} \}_{K2}$	Double-DES	112 Bit Key
$\{ \{ \{ m \}_{K1} \}_{K2} \}_{K3}$	Triple-DES	168 Bit Key

Single-DES Mode: K1 = K2 ≠ K3

$$\{ \{ \{ m \overset{E}{\}}_{K1} \overset{D}{\}}_{K1} \overset{E}{\}}_{K3}$$

$$\{ \quad m \quad \}_{K3}$$

Week 7

Triple-DES

$\{ m \}_{K1}$	Single-DES	56 Bit Key
$\{ \{ m \}_{K1} \}_{K2}$	Double-DES	112 Bit Key
$\{ \{ \{ m \}_{K1} \}_{K2} \}_{K3}$	Triple-DES	168 Bit Key

Single-DES Mode: K1 = K2 ≠ K3

$$\{ \{ \{ m \overset{E}{\}}_{K1} \overset{D}{\}}_{K1} \overset{E}{\}}_{K3}$$

$$\{ \quad m \quad \}_{K3}$$

Triple-DES Mode: K1 = K3 ≠ K2

Effective 112 bits

$$\underset{E}{\{} \underset{D}{\{} \underset{E}{\{} m \}_{K1} \}_{K2} \}_{K1}$$

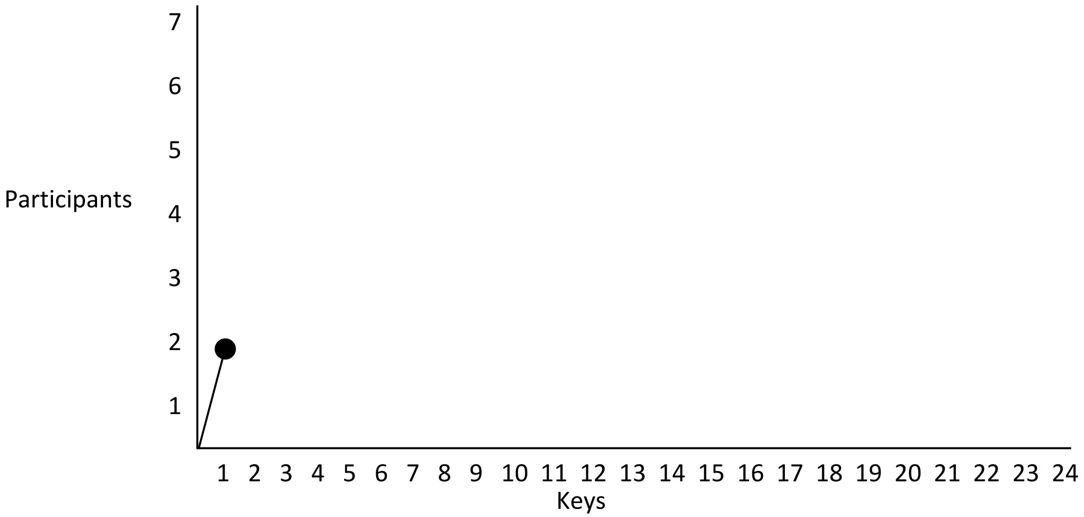
E D E Mode

What is the Scaling Issue for Conventional Cryptography?

Week 7

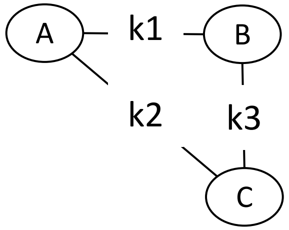
Conventional Encryption Scaling Issue

2 participants – 1 shared key



Week 7

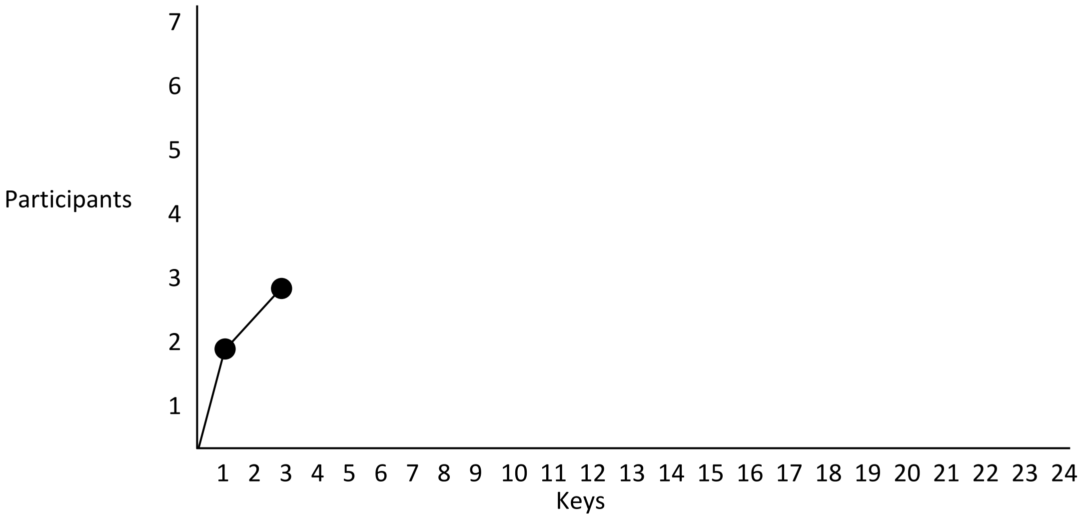
Conventional Encryption Scaling Issue



2 participants – 1 shared key

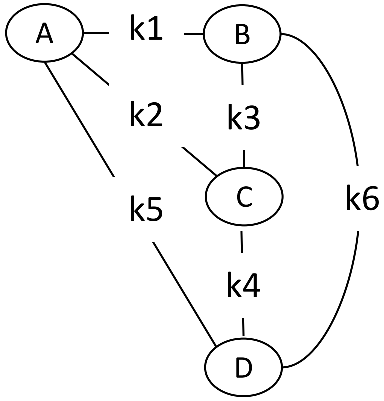
3 participants – 3 shared keys

Added participant 1
Added new keys 2



Week 7

Conventional Encryption Scaling Issue

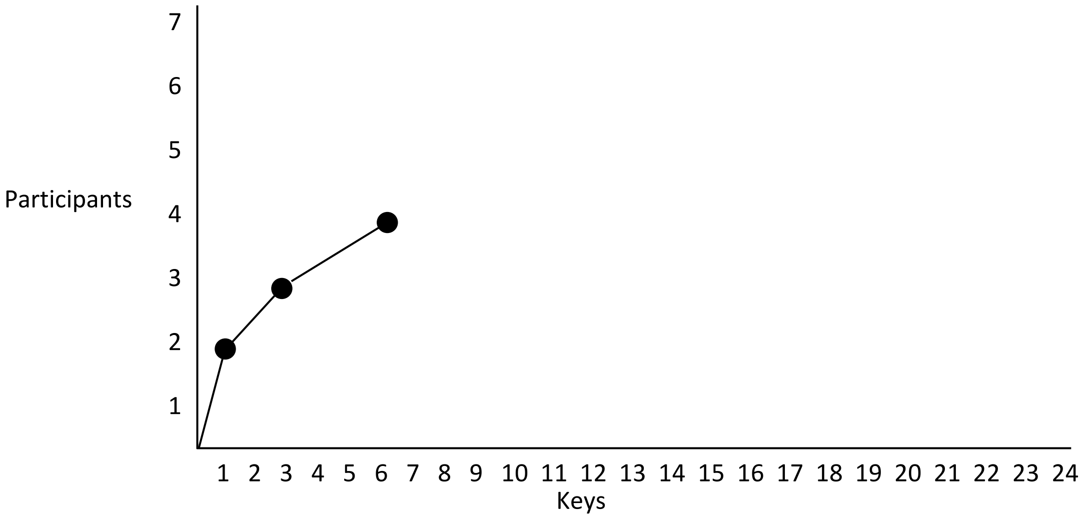


2 participants – 1 shared key

3 participants – 3 shared keys

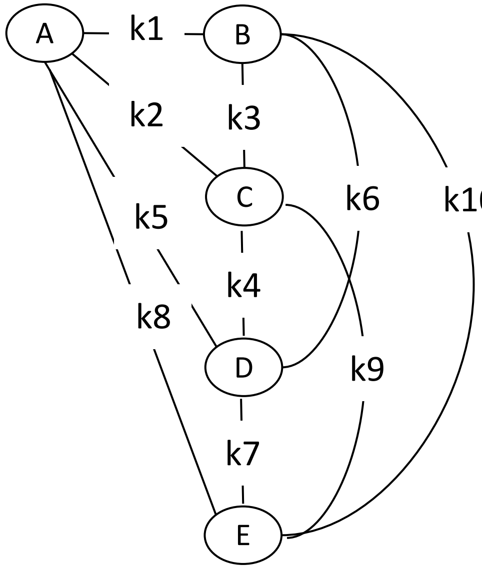
4 participants – 6 shared keys

Added participant 1
Added new keys 3



Week 7

Conventional Encryption Scaling Issue



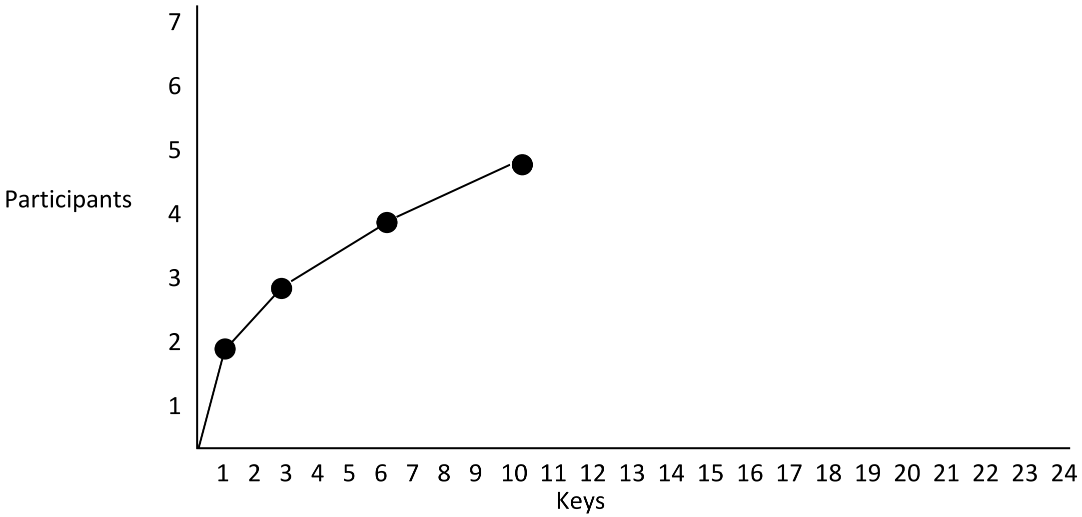
2 participants – 1 shared key

3 participants – 3 shared keys

4 participants – 6 shared keys

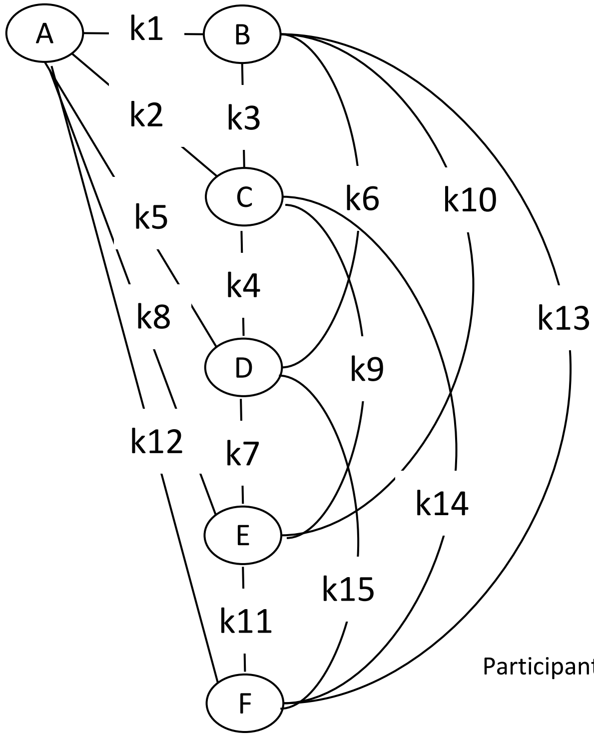
5 participants – 10 shared keys

Added participant 1
Added new keys 4



Week 7

Conventional Encryption Scaling Issue



2 participants – 1 shared key

3 participants – 3 shared keys

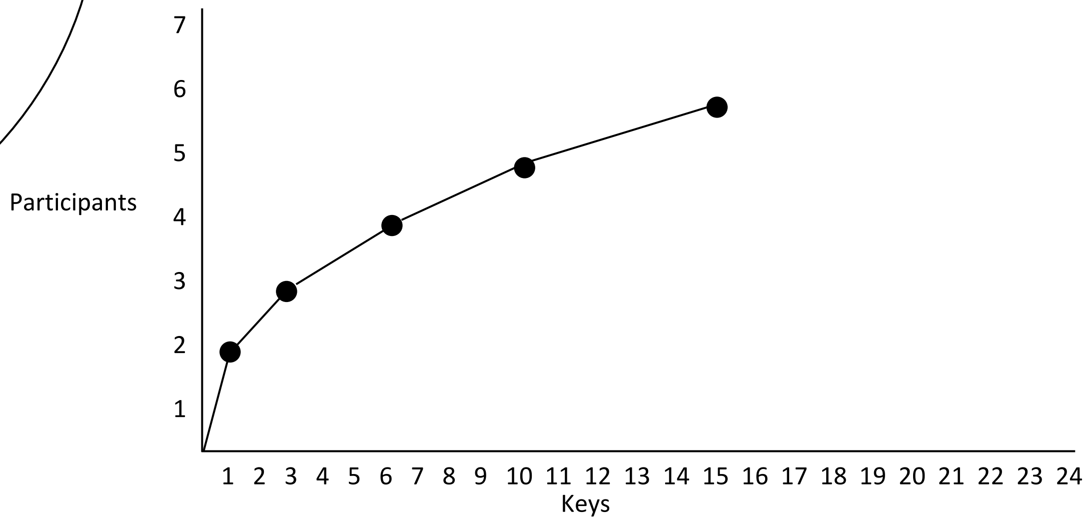
4 participants – 6 shared keys

5 participants – 10 shared keys

6 participants – 15 shared keys

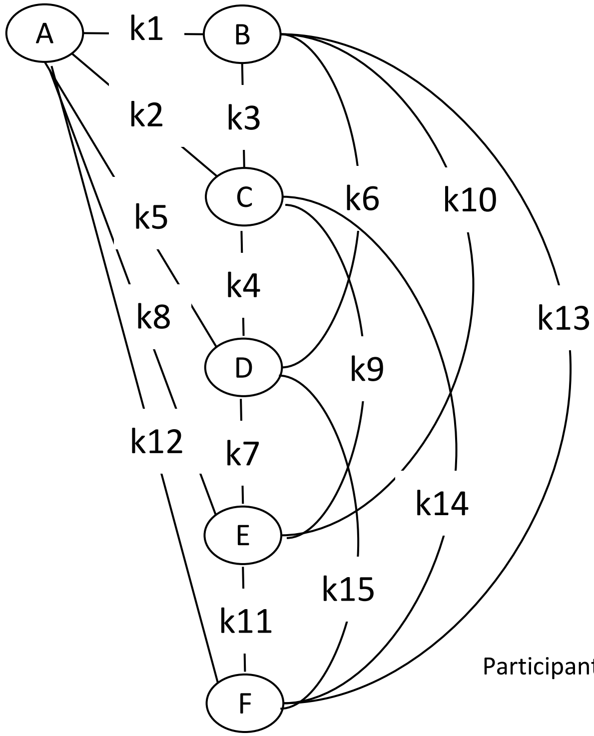
Added participant 1

Added new keys 5



Week 7

Conventional Encryption Scaling Issue



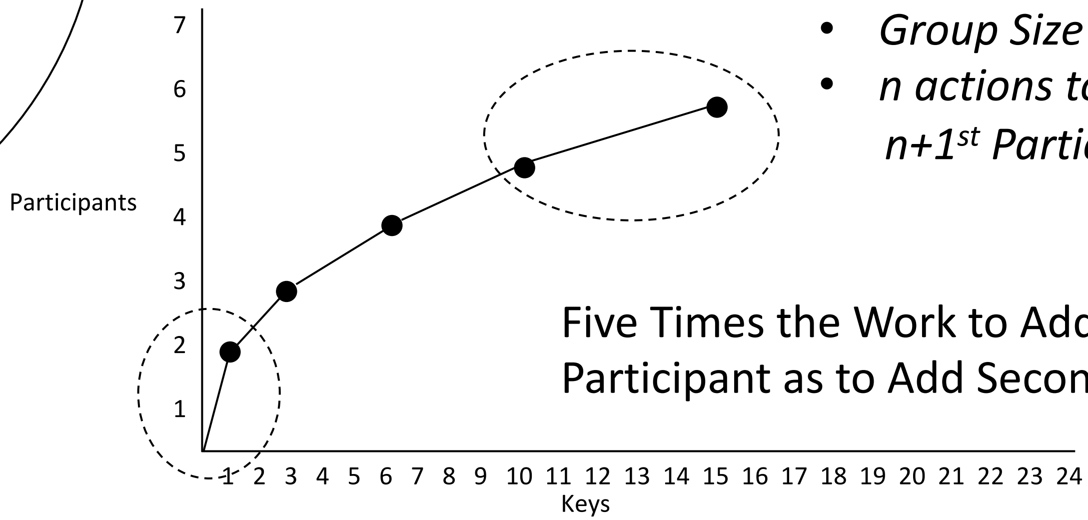
2 participants – 1 shared key

3 participants – 3 shared keys

4 participants – 6 shared keys

5 participants – 10 shared keys

6 participants – 15 shared keys



- *Group Size = n*
- *n actions to add n+1st Participant*

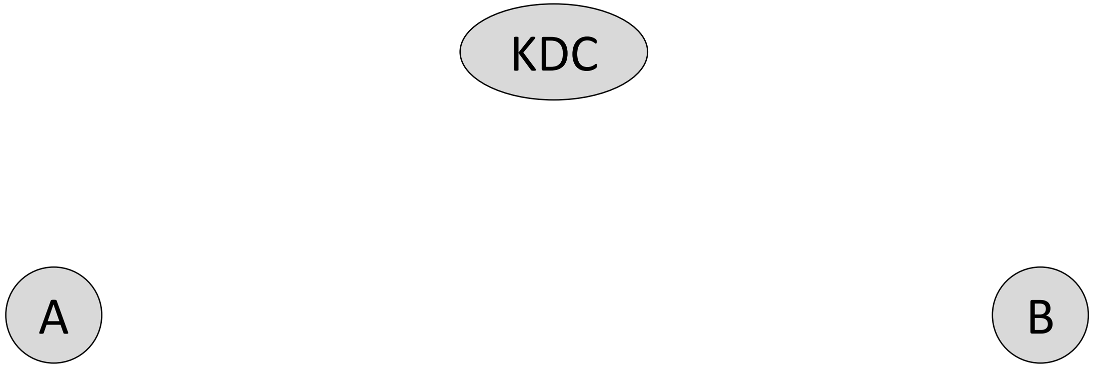
Five Times the Work to Add Sixth Participant as to Add Second

Added participant 1
Added new keys 5

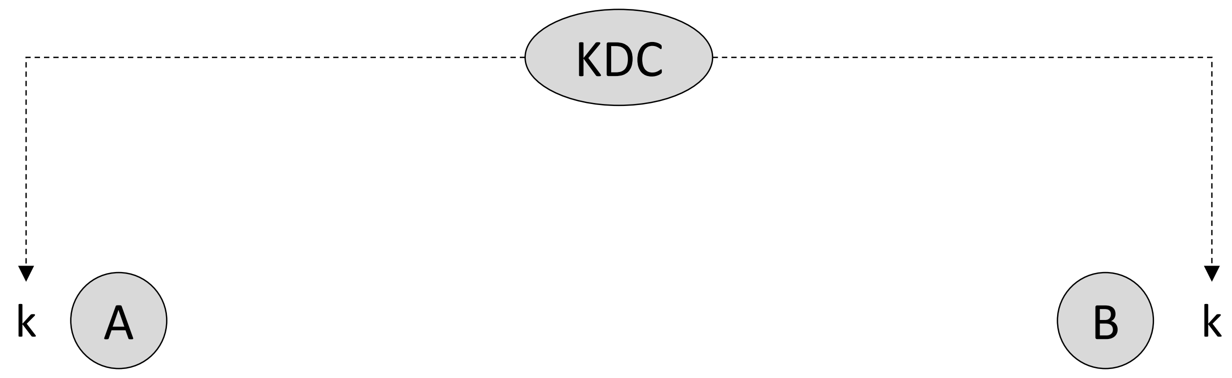
What are the Key Security Properties of Conventional Cryptography?

Week 7

Conventional Cryptography

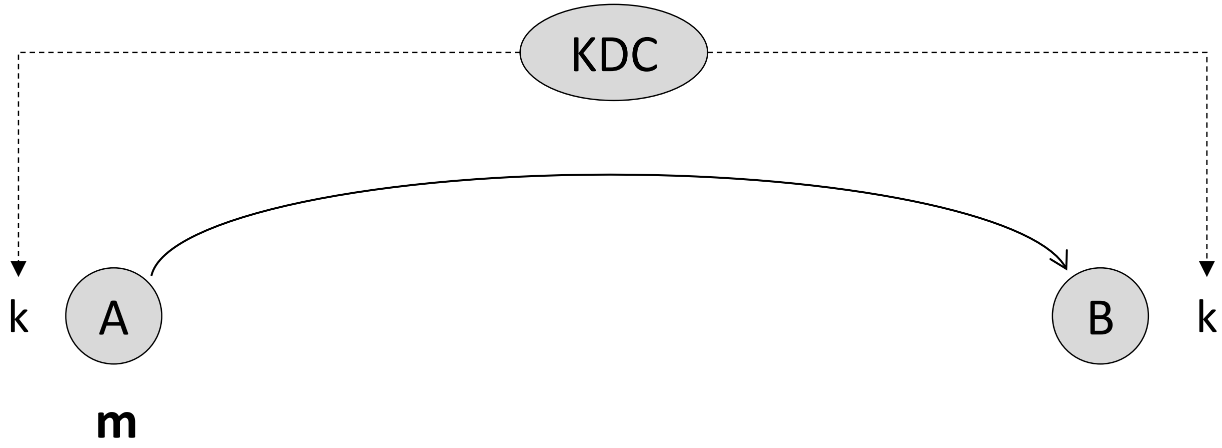


Conventional Cryptography



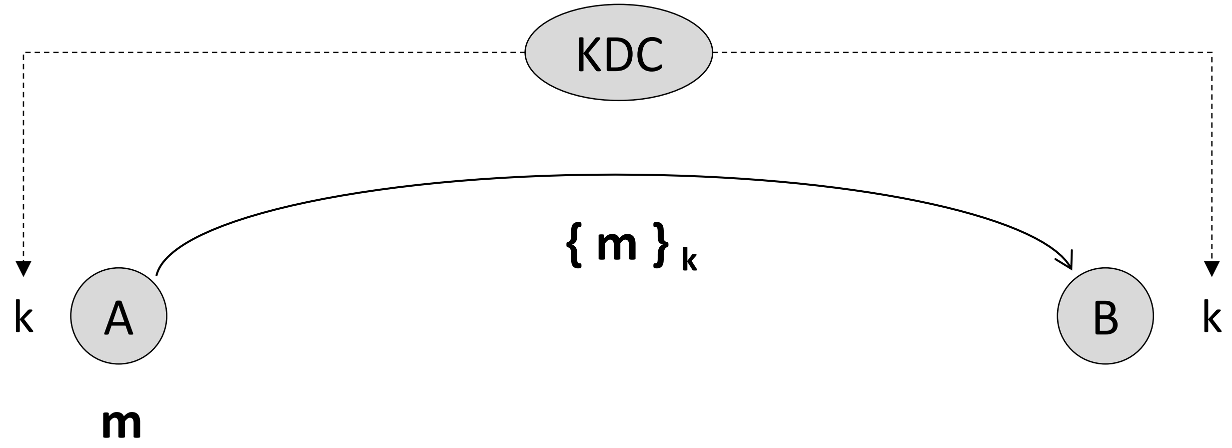
Week 7

Conventional Cryptography



Alice creates message m . . .

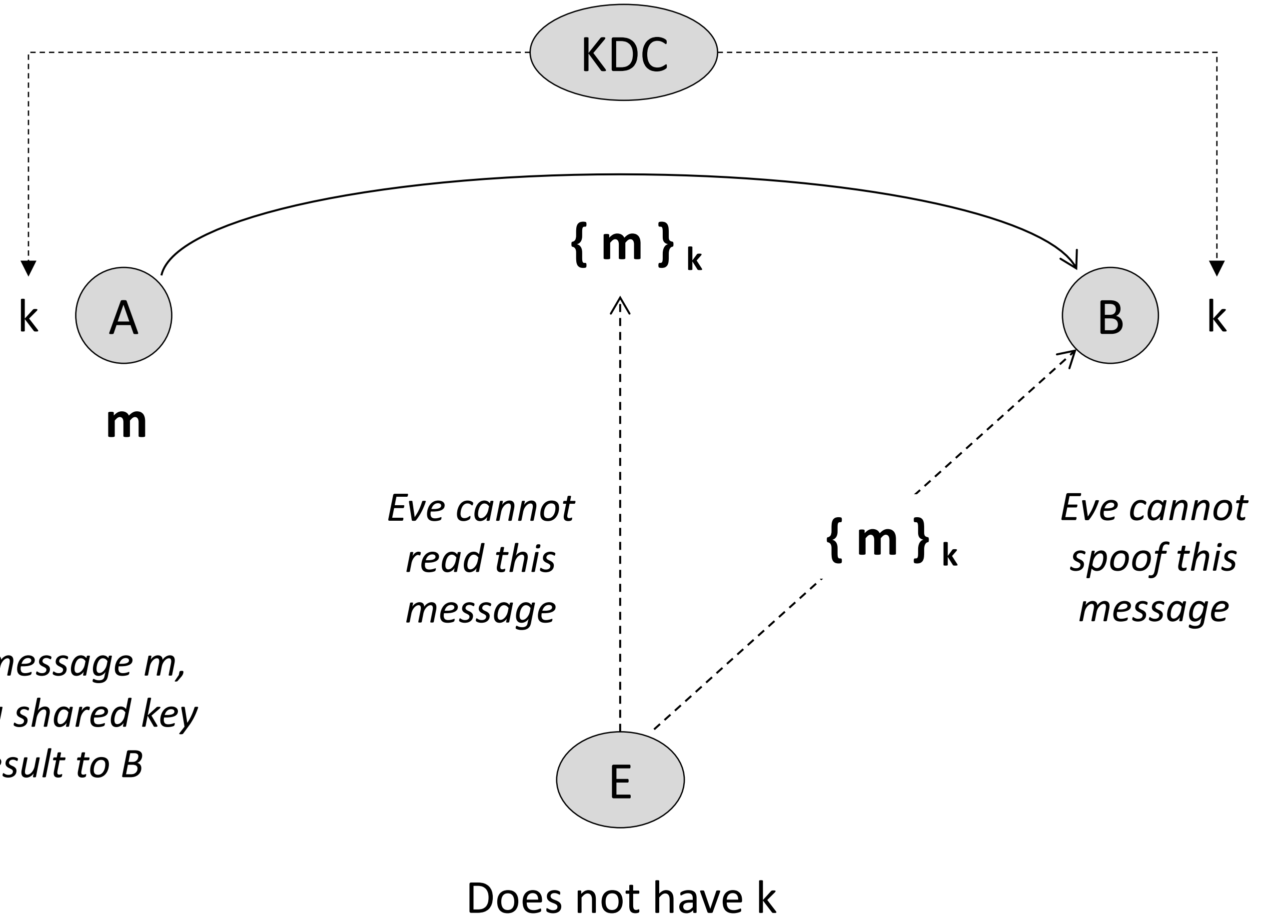
Conventional Cryptography



Alice creates message m, encrypts using shared key k and sends result to B

Week 7

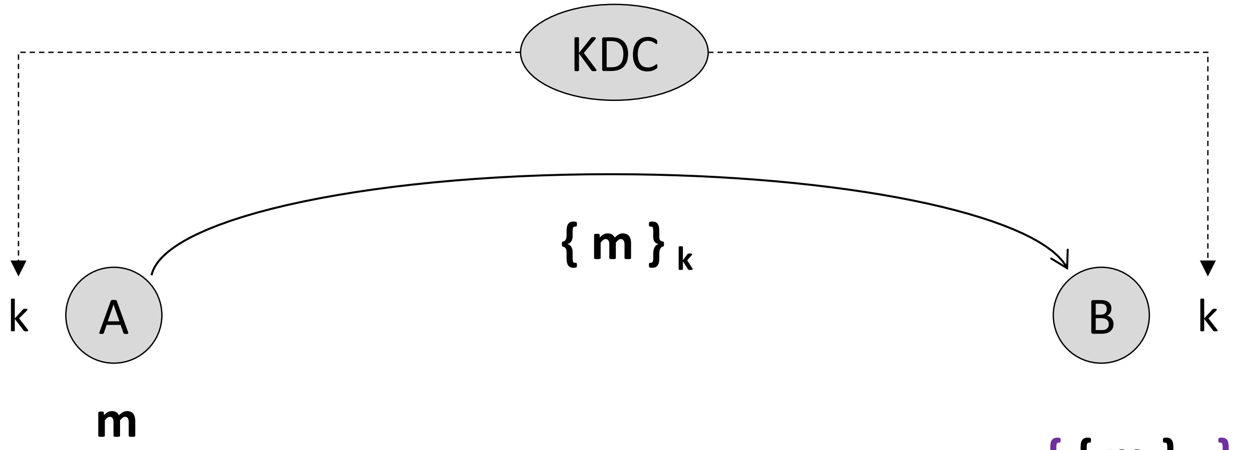
Conventional Cryptography



Alice creates message m, encrypts using shared key k and sends result to B

Week 7

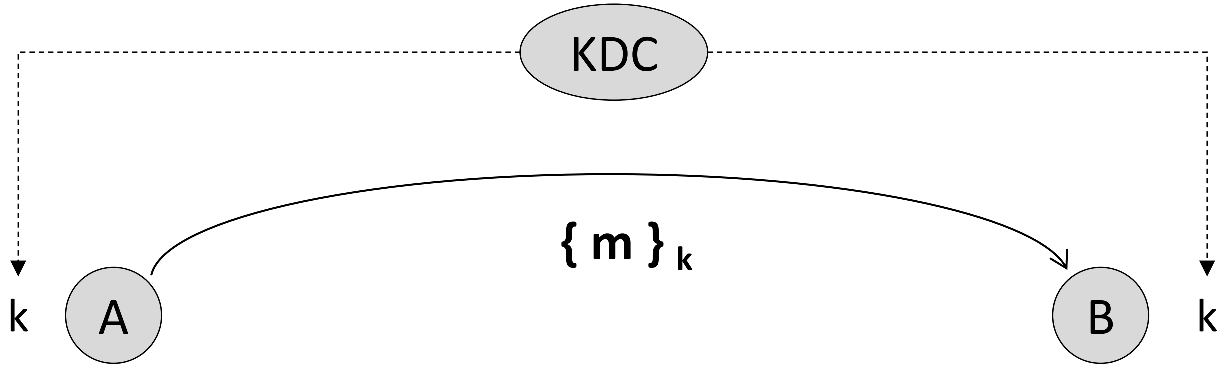
Conventional Cryptography



$$\{\{m\}_k\}_k = m$$

Bob receives encrypted message, and decrypts using shared key k and obtains message m

Conventional Cryptography

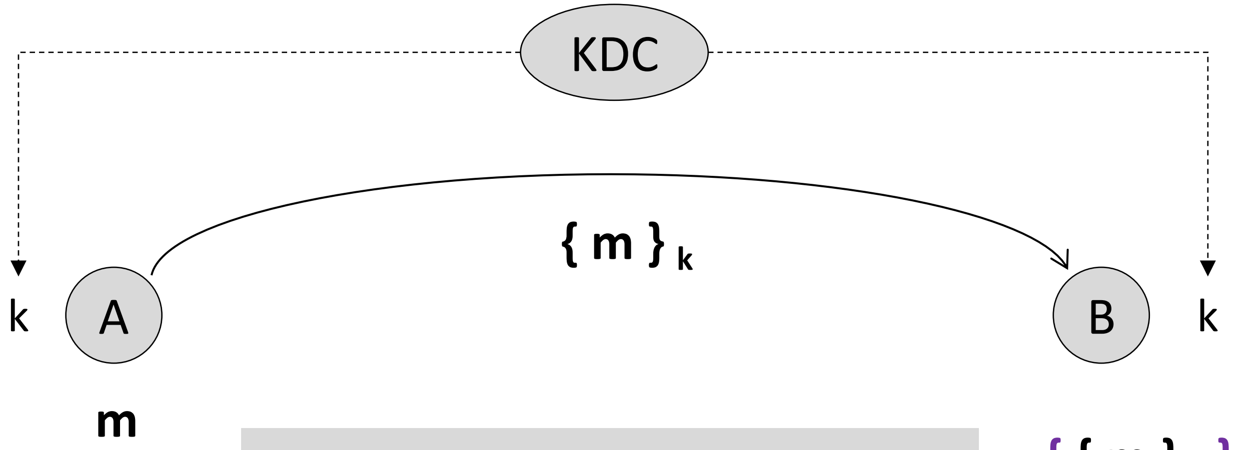


m

Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{ \{ m \}_k \}_k = m$

Conventional Cryptography



Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{\{m\}_k\}_k = m$

Does this approach scale? **NO**

How Does Block Chaining Work?

Conventional Block Cryptography – Covert Channel

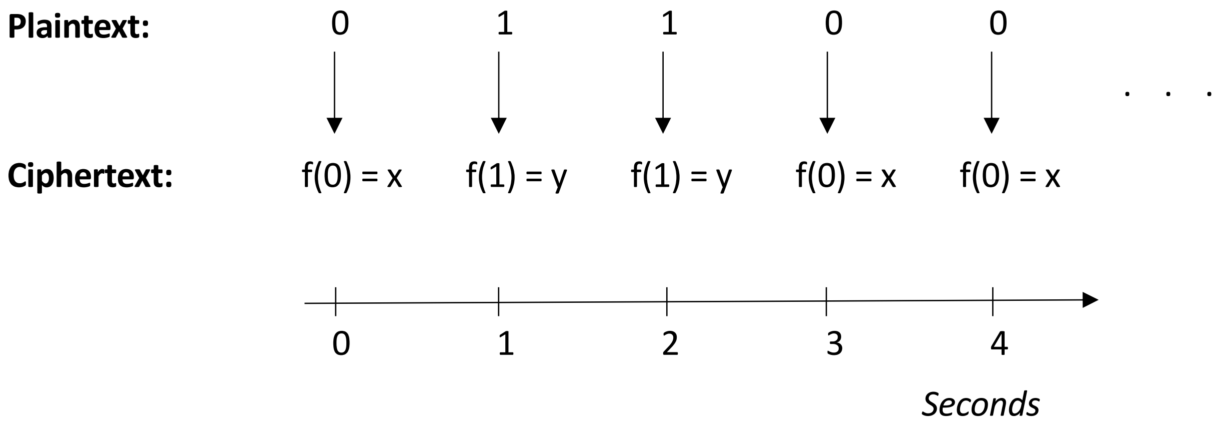
Blocks Fixed by Sender into a Pattern

Plaintext: Ʊ Σ Σ Ʊ Ʊ Σ Σ . . .

Ciphertext: f(Ʊ) f(Σ) f(Σ) f(Ʊ) f(Ʊ) f(Σ) f(Σ)

Pattern Can Emerge for External Observer in Encrypted Data

Conventional Block Cryptography – 1 bps Channel



Week 7

Block Chain Mode Cryptography – Circa 1976 at IBM

Patents

Find prior art | Discuss this patent

Message verification and transmission error detection by block chaining

US 4074066 A

Publication number	US4074066 A
Publication type	Grant
Application number	US 05/680,404
Publication date	Feb 14, 1978
Filing date	Apr 26, 1976
Priority date ?	Apr 26, 1976
Also published as	CA1100588A, CA1100588A1, DE2715631A1, DE2715631C2
Inventors	William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman
Original Assignee	International Business Machines Corporation
Export Citation	BiBTeX, EndNote, RefMan

Patent Citations (5), Referenced by (52), Classifications (10)

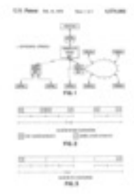
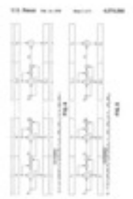
External Links: USPTO, USPTO Assignment, Espacenet

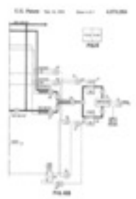
ABSTRACT

A message transmission system for the secure transmission of multi-block data messages from a sending station to a receiving station.

The sending station contains cryptographic apparatus operative in successive cycles of operation during each of which an input block of clear data bits is ciphered under control of an input set of cipher key bits to generate an output block of ciphered data bits for transmission to the receiving station. Included in the cryptographic apparatus of the sending station is means providing one of the inputs for each succeeding ciphering cycle of operation as a function of each preceding ciphering cycle of operation. As a result, each succeeding output block of ciphered data bits is effectively chained to all preceding cycles of operation of the cryptographic apparatus of the sending station and is a function of the corresponding input block of clear data bits, all preceding input blocks of clear data bits and the initial input set of cipher key bits.

IMAGES (5)




Week 7

Block Chain Mode Cryptography

Genesis Block

Plaintext: G

$\downarrow$

Ciphertext: $f(G) = c_1$

Week 7

Block Chain Mode Cryptography

Genesis Block

Plaintext: G 1

Ciphertext: $f(G) = c_1$ $f(c_1, 1)) = c_2$

Week 7

Block Chain Mode Cryptography

Genesis Block

Plaintext: G ↓ 1 ↓ 1 ↓

Ciphertext: $f(G) = c_1$ $f(c_1, 1)) = c_2$ $f(c_2, 1) = c_3$

Week 7

Block Chain Mode Cryptography

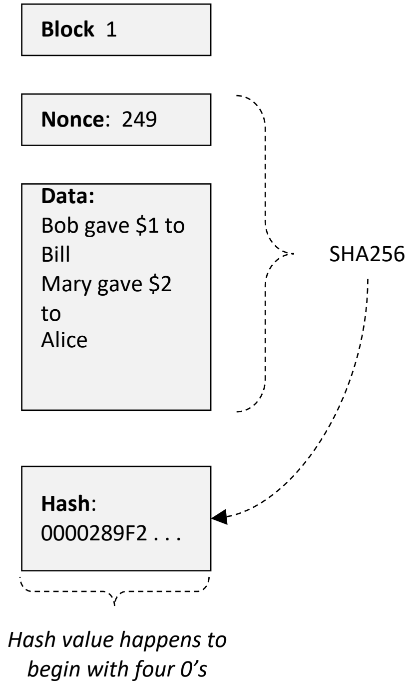
Genesis Block

Plaintext: G 1 1 0 . . .

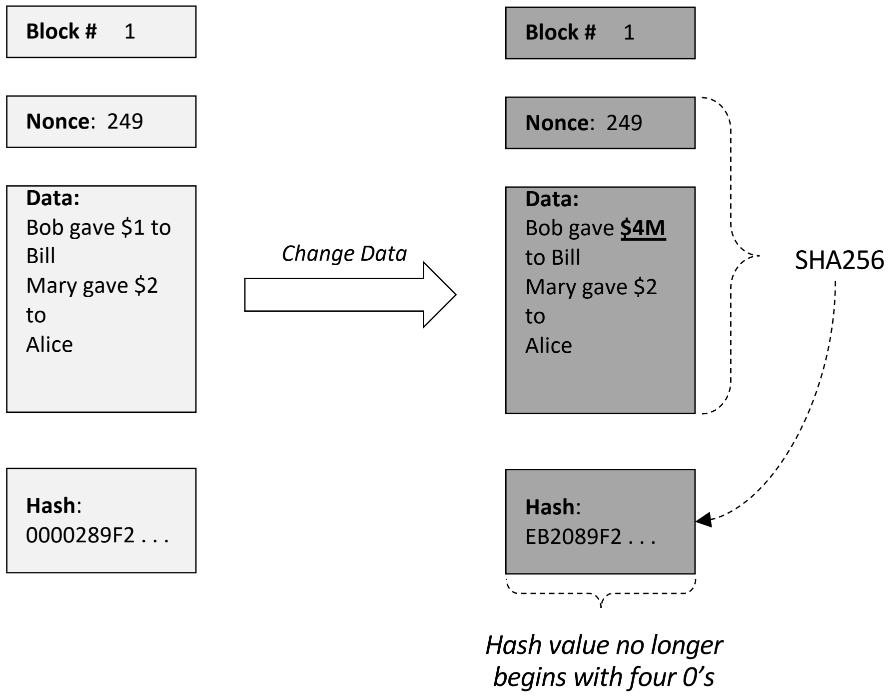
Ciphertext: $f(G) = c_1$ $f(c_1, 1)) = c_2$ $f(c_2, 1) = c_3$ $f(c_3, 0) = c_4$

Week 7

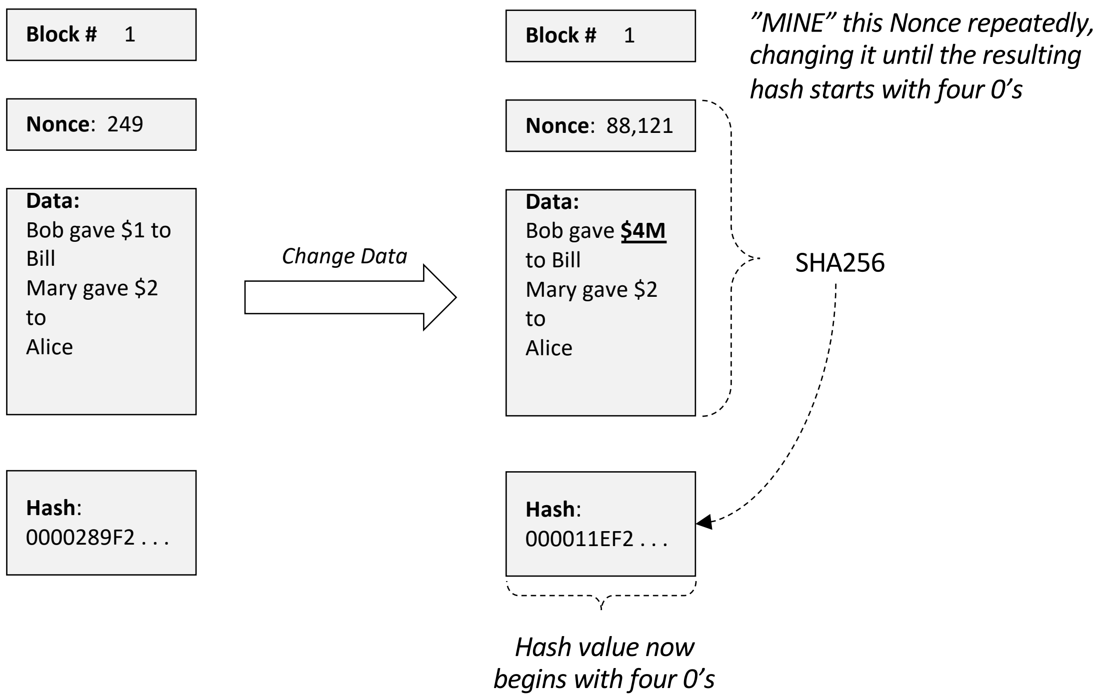
Modern Block Chain Usage



Modern Block Chain Usage



Modern Block Chain Usage



Week 7

Modern Block Chain Usage

Block # 1

Nonce: 249

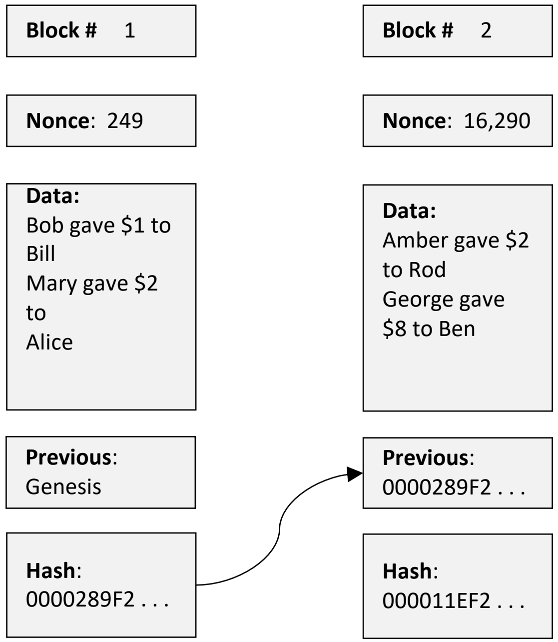
Data:
Bob gave $1 to Bill
Mary gave $2 to Alice

Previous: Genesis

Hash: 0000289F2 . . .

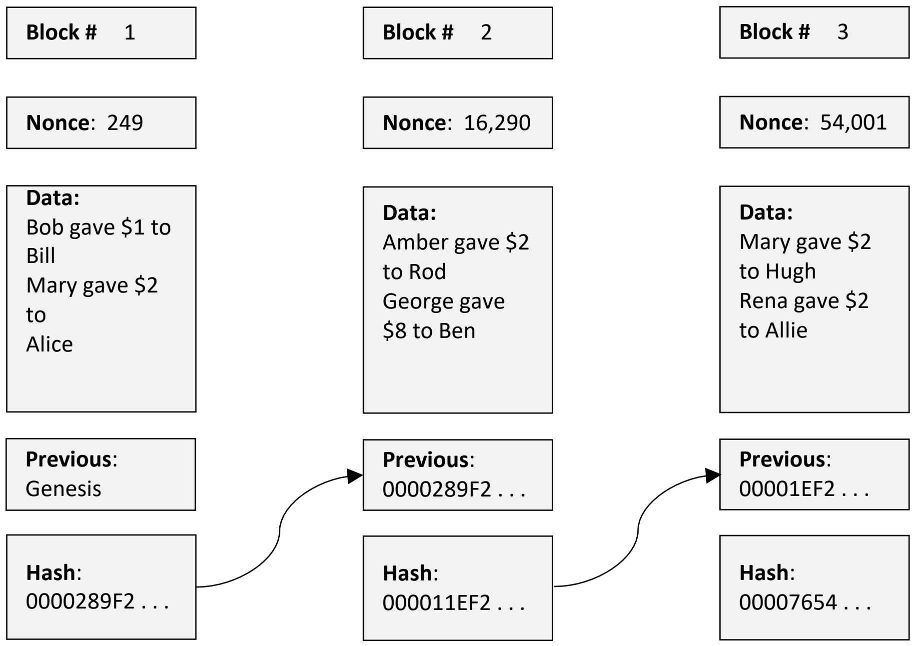
Week 7

Modern Block Chain Usage



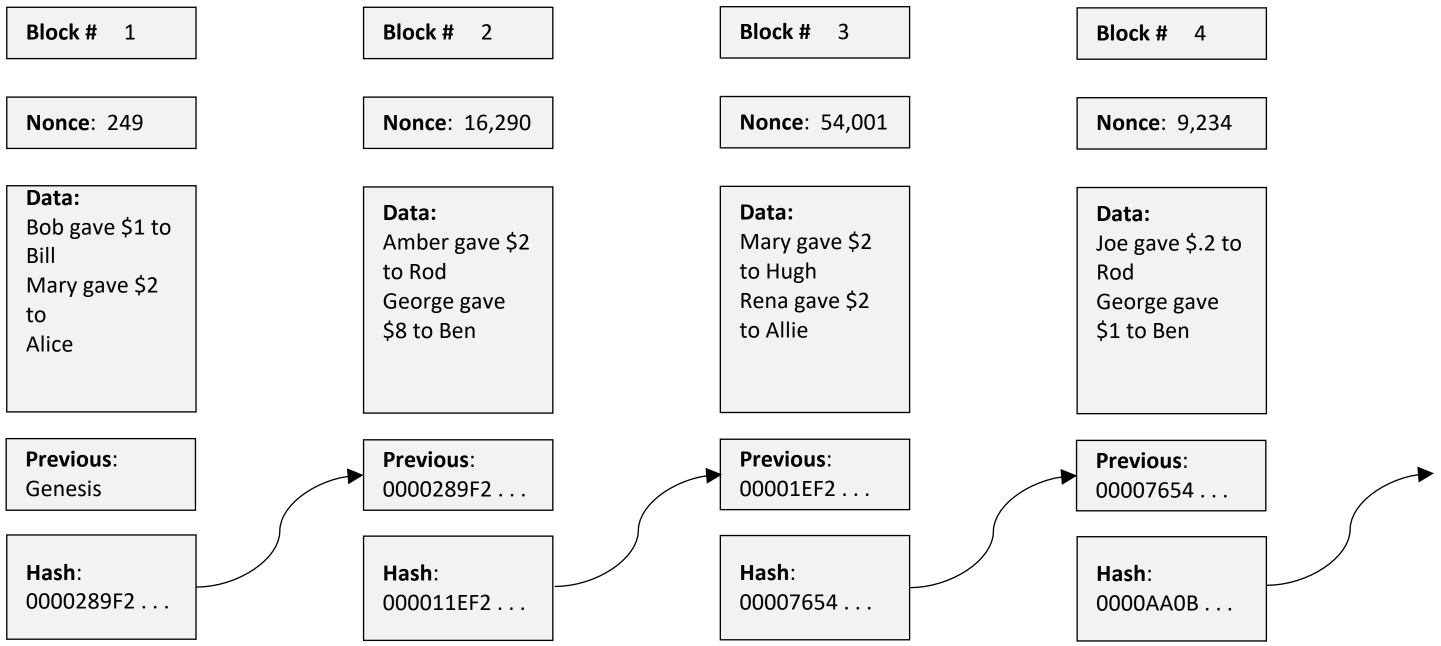
Week 7

Modern Block Chain Usage



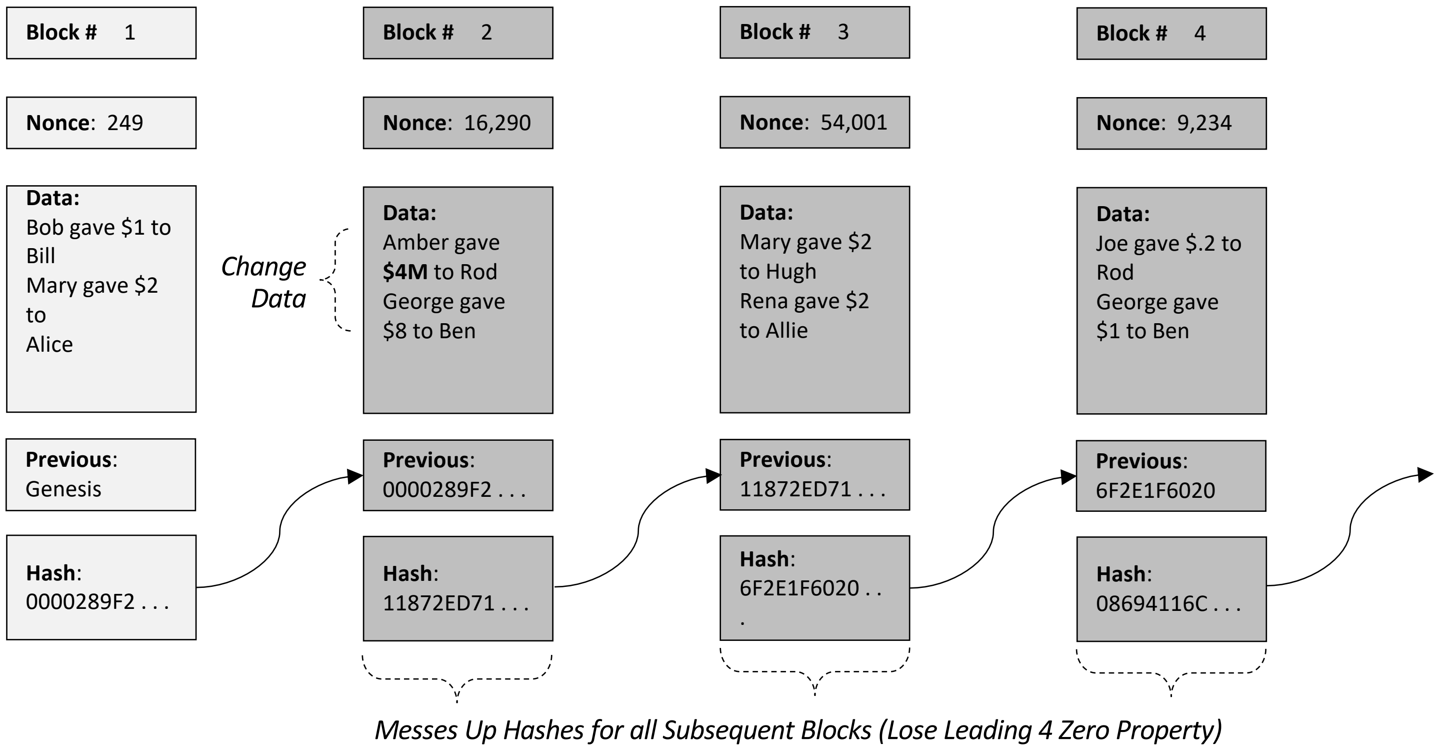
Week 7

Modern Block Chain Usage



Week 7

Modern Block Chain Usage



Week 7

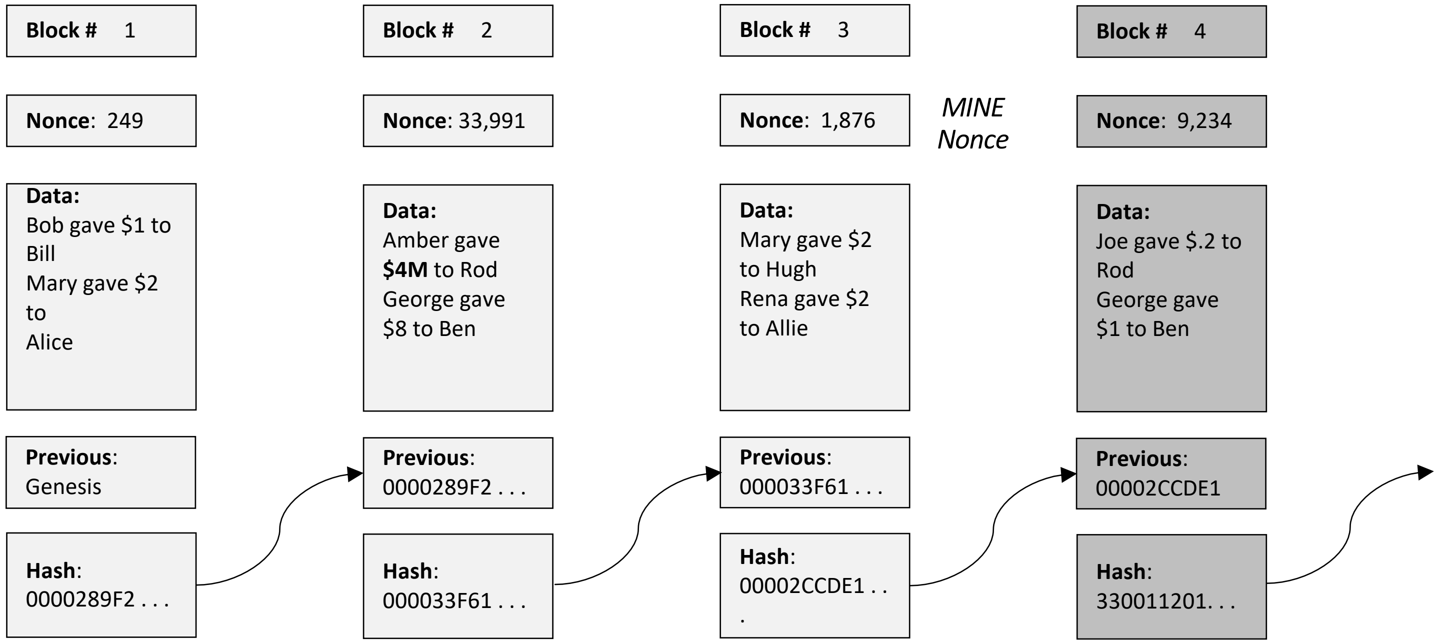
Modern Block Chain Usage

Block # 1	**Block #** 2	**Block #** 3	**Block #** 4
Nonce: 249	**Nonce**: 33,991	**Nonce**: 54,001	**Nonce**: 9,234
Data: Bob gave $1 to Bill Mary gave $2 to Alice	**Data:** Amber gave **$4M** to Rod George gave $8 to Ben	**Data:** Mary gave $2 to Hugh Rena gave $2 to Allie	**Data:** Joe gave $.2 to Rod George gave $1 to Ben
Previous: Genesis	**Previous**: 0000289F2 . . .	**Previous**: 000033F61 . . .	**Previous**: 813457719
Hash: 0000289F2 . . .	**Hash**: 000033F61 . . .	**Hash**: 813457719 . . .	**Hash**: FFCDE2216. . .

MINE Nonce

Week 7

Modern Block Chain Usage



Week 7

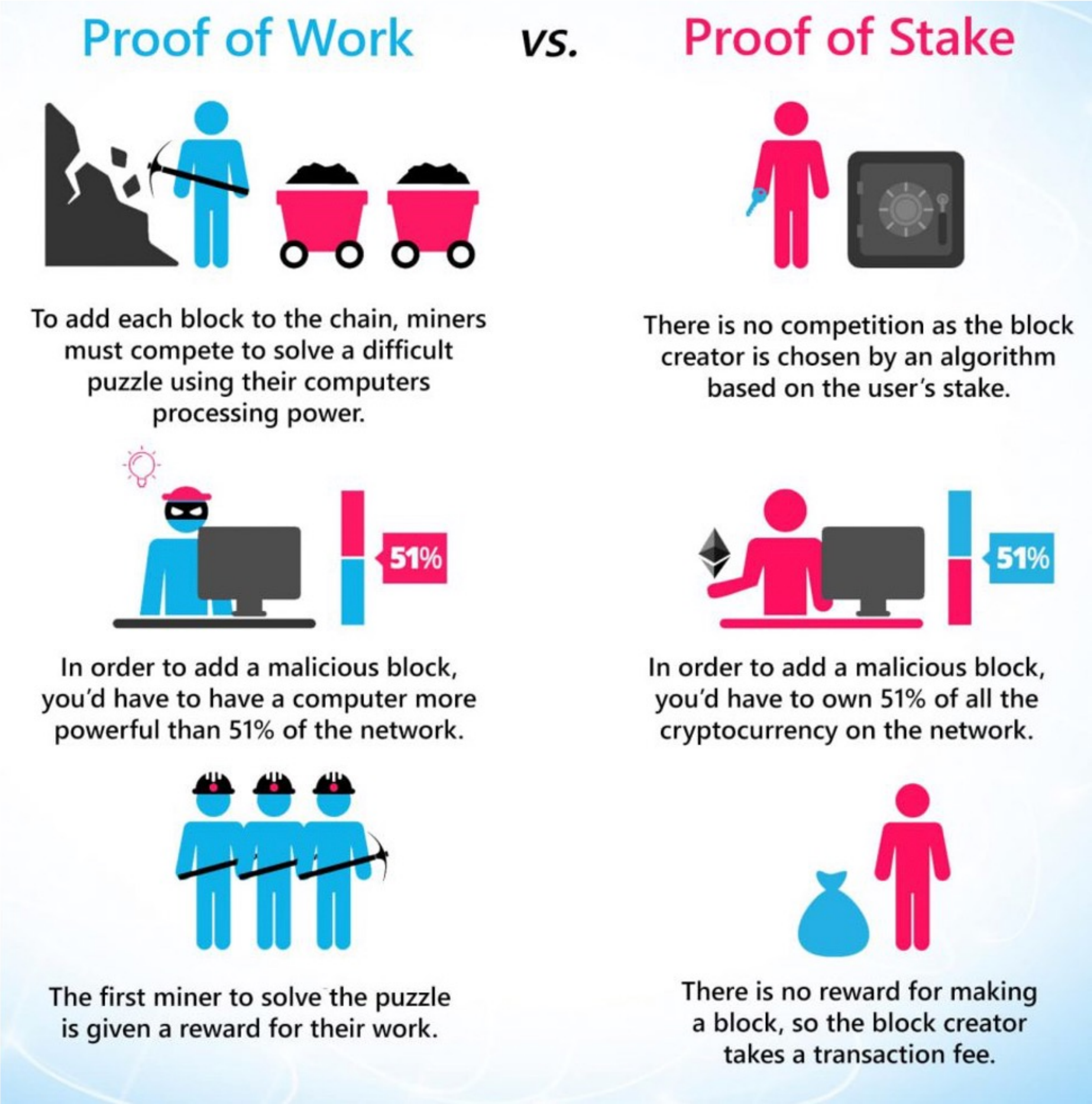
Modern Block Chain Usage

Block # 1	**Block #** 2	**Block #** 3	**Block #** 4
Nonce: 249	**Nonce**: 33,991	**Nonce**: 1,876	**Nonce**: 128
Data: Bob gave $1 to Bill Mary gave $2 to Alice	**Data:** Amber gave **$4M** to Rod George gave $8 to Ben	**Data:** Mary gave $2 to Hugh Rena gave $2 to Allie	**Data:** Joe gave $.2 to Rod George gave $1 to Ben
Previous: Genesis	**Previous**: 0000289F2 . . .	**Previous**: 000033F61 . . .	**Previous**: 00002CCDE1
Hash: 0000289F2 . . .	**Hash**: 000033F61 . . .	**Hash**: 00002CCDE1 . . .	**Hash**: 000067BC32. . .

MINE Nonce

Week 7

Week 7



Proof of Work
vs.
Proof of Stake
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.
There is no competition as the block creator is chosen by an algorithm based on the user's stake.
51%
51%
In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.
In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.
The first miner to solve the puzzle is given a reward for their work.
There is no reward for making a block, so the block creator takes a transaction fee.