Week 6

Lamport S/Key Protocol – Purpose

A

B

A is reporting its identity to B

B is attempting to validate A's reported identity (i.e., authenticating A)

Lamport S/Key Protocol – Set-Up

A

B

Known Function:

f: integer -> integer

Known Seed:

integer λ

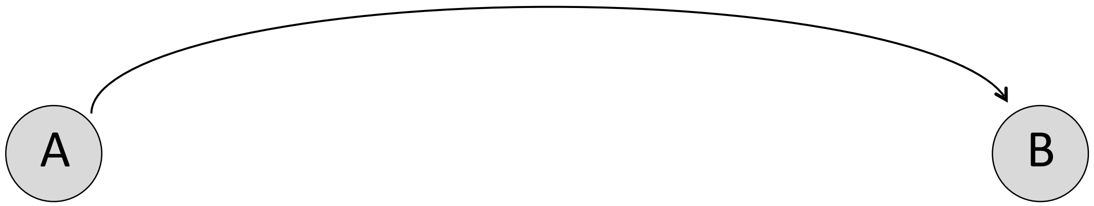
Number of Rounds:

n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**
C	**f’, n, $f'^{\,n}(\lambda')$**
G	**f’’, n, $f''^{\,n}(\lambda'')$**
. . .	. . .

Lamport S/Key Protocol

Step 1: I am Alice



Known Function:

f: integer -> integer

Known Seed:

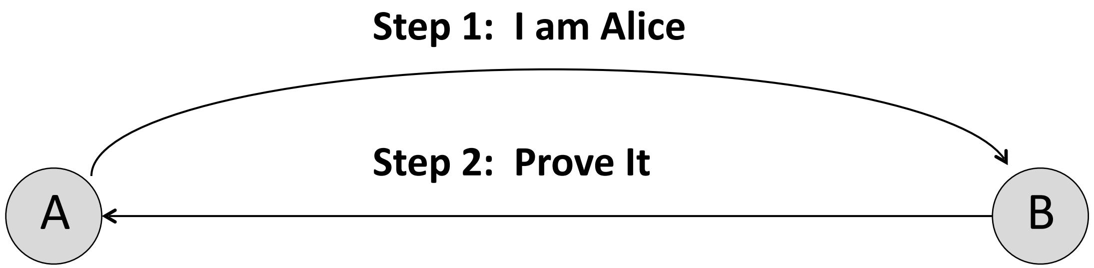
integer λ:

Number of Rounds:

n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**

Lamport S/Key Protocol

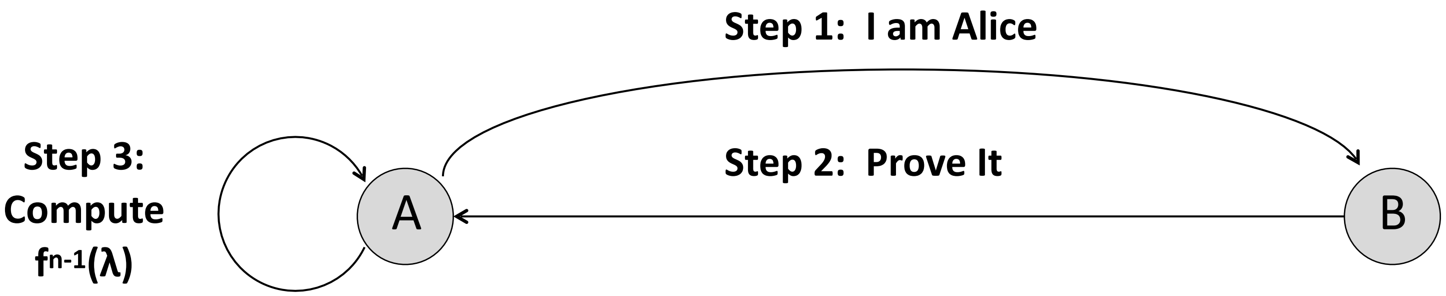


Known Function:
f: integer -> integer
Known Seed:
integer λ
Number of Rounds:
n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**

Week 6

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

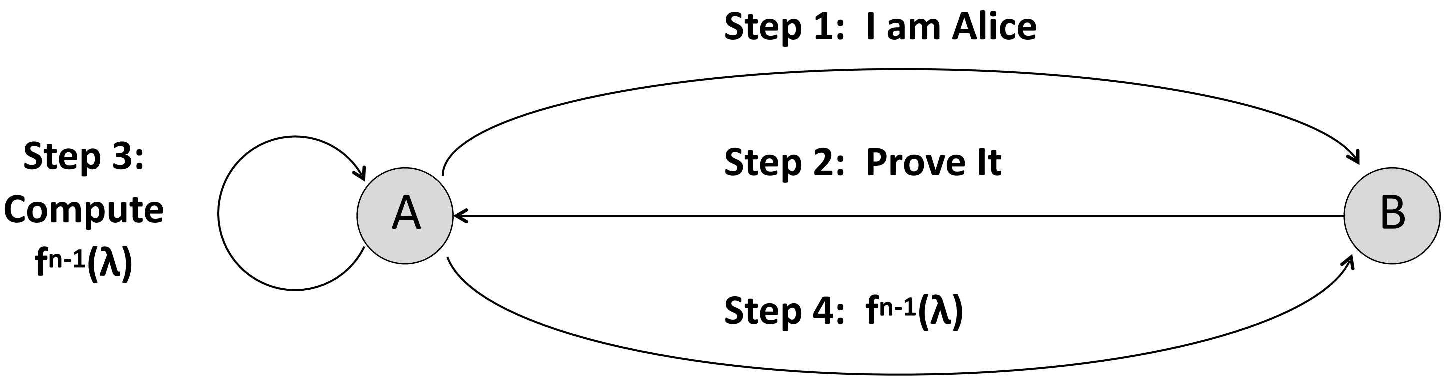
integer λ

Number of Rounds:

n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

integer λ

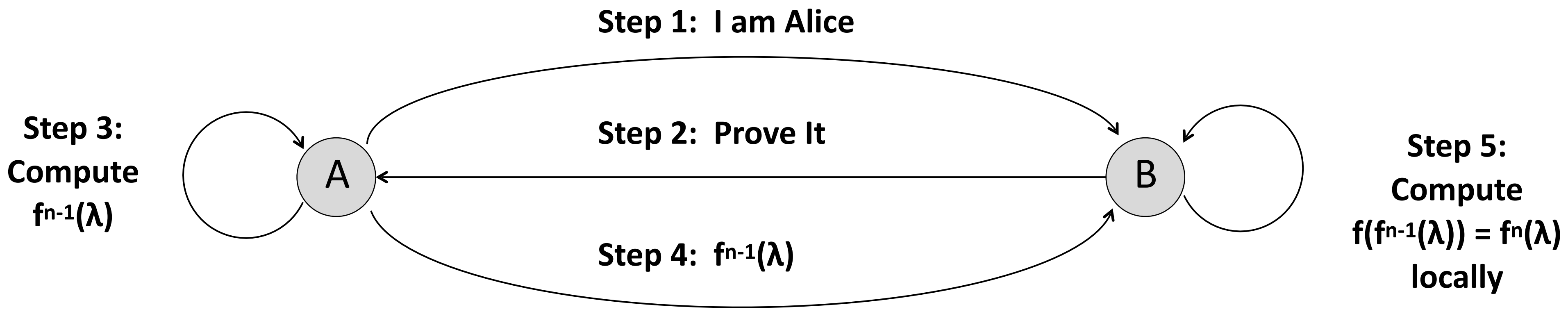
Number of Rounds:

n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**

Week 6

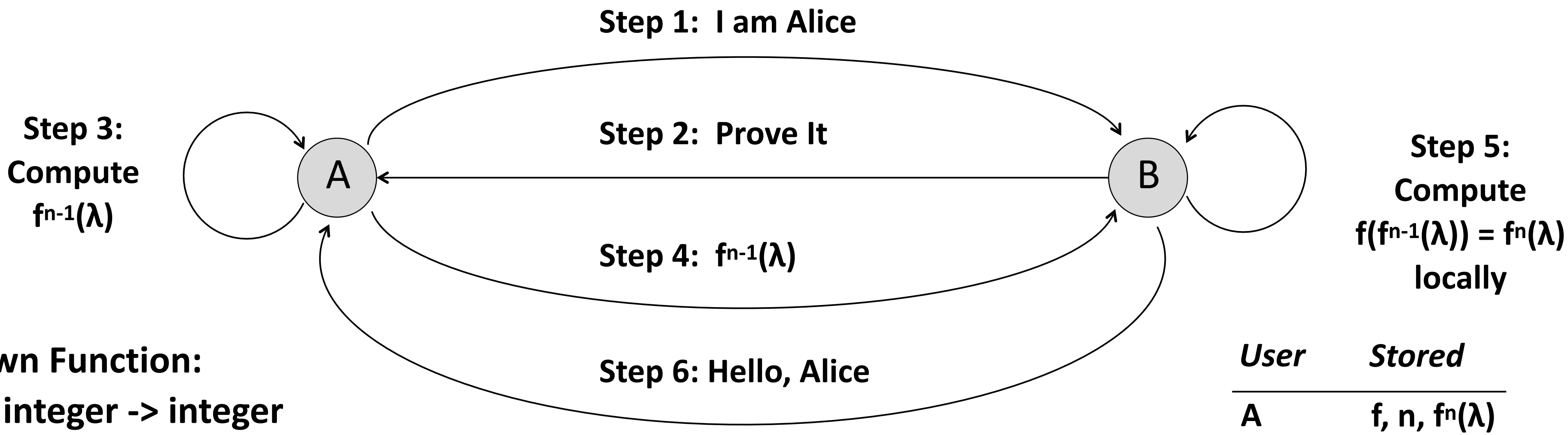
Lamport S/Key Protocol



Known Function:
f: integer -> integer
Known Seed:
integer λ
Number of Rounds:
n = 10,000

User	*Stored*
A	**f, n, $f^{n}(\lambda)$**

Lamport S/Key Protocol



User	*Stored*
A	**f, n, $f^{n}(\lambda)$**

Known Function:

f: integer -> integer

Known Seed:

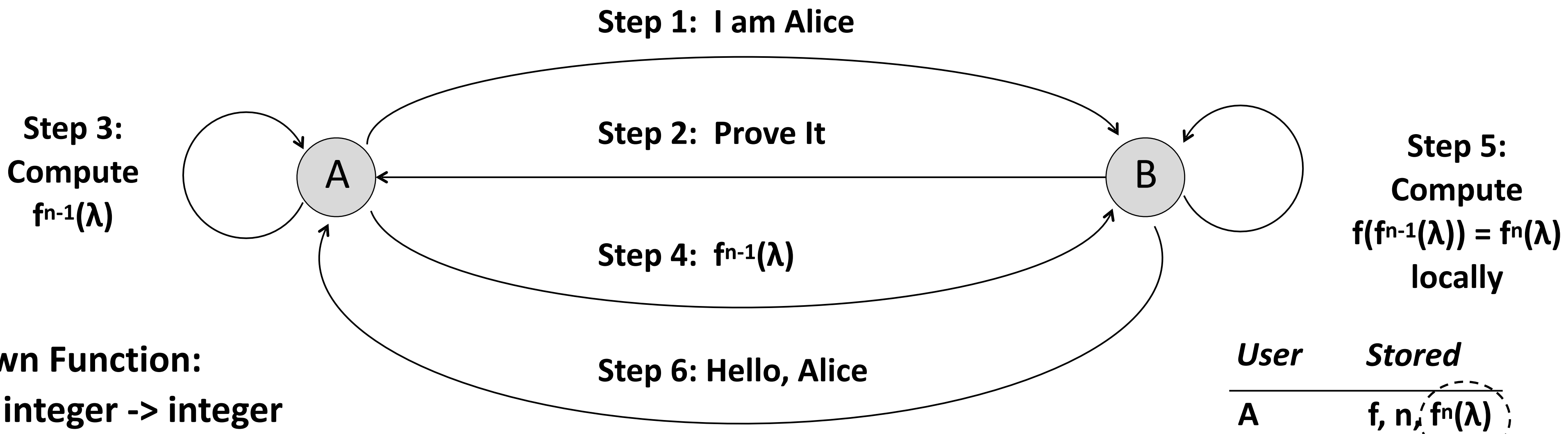
integer λ

Number of Rounds:

n = 10,000

Week 6

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

integer λ

Number of Rounds:

n = 10,000

User	*Stored*
A	**f, n, $f^n(\lambda)$**

$f^n(\lambda)$ stored

Lamport S/Key Protocol

A

B

Known Function:

f: integer -> integer

Known Seed:

integer λ

Number of Rounds:

n-1 = 9,999

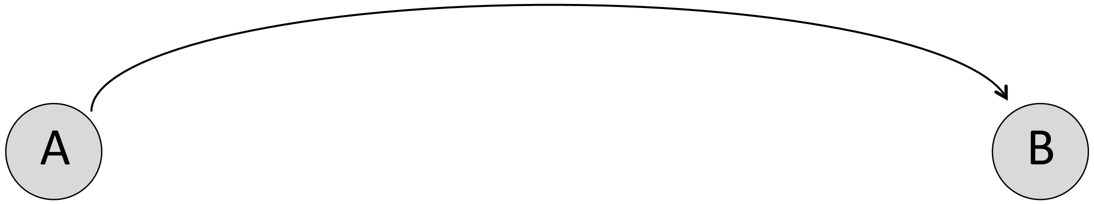
User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

$f^{n-1}(\lambda)$
now stored

Week 6

Lamport S/Key Protocol

Step 1: I am Alice



Known Function:

f: integer -> integer

Known Seed:

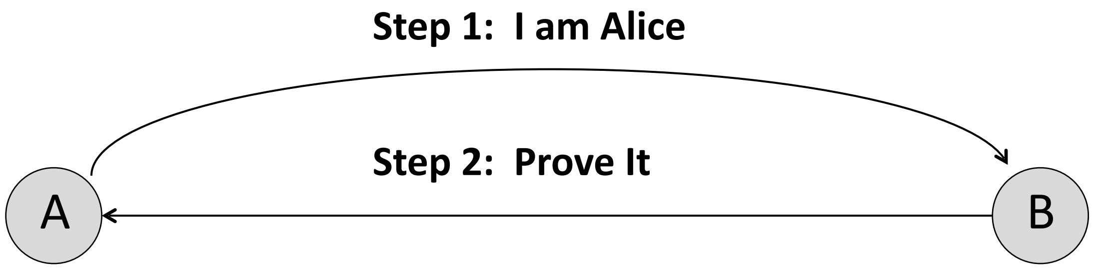
integer λ

Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

integer λ

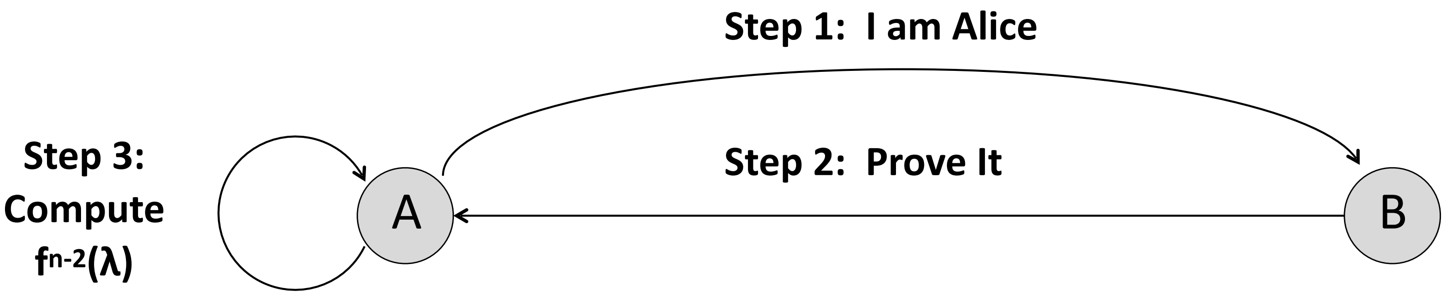
Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Week 6

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

integer λ

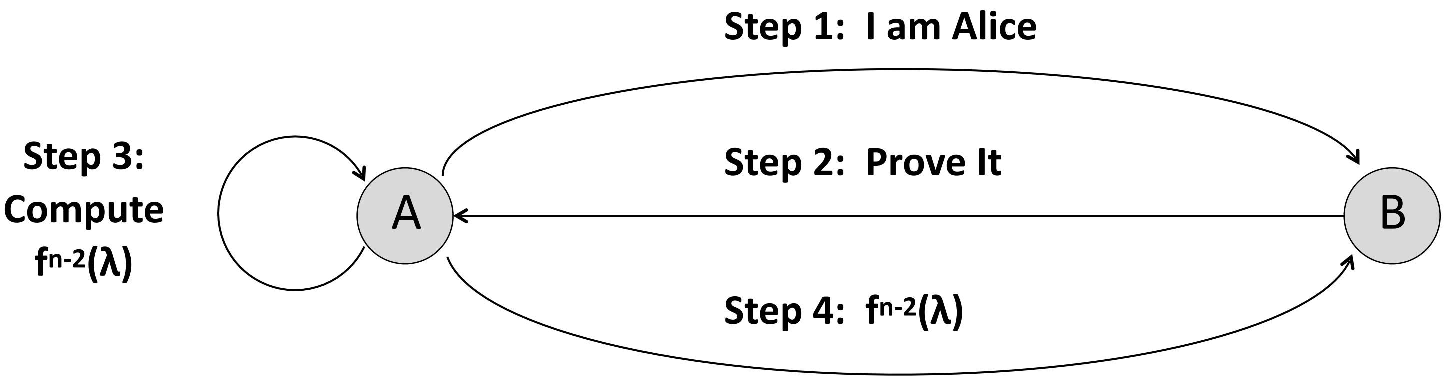
Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Week 6

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

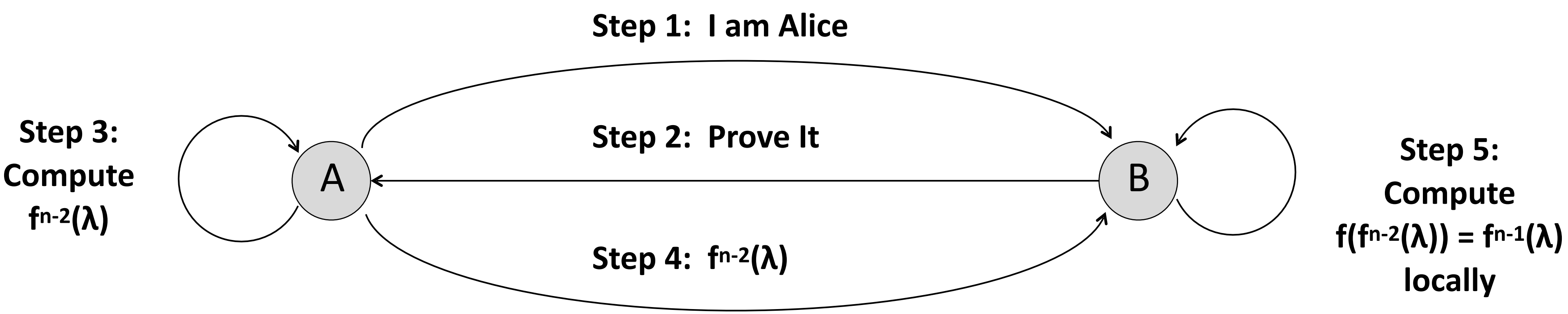
integer λ

Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

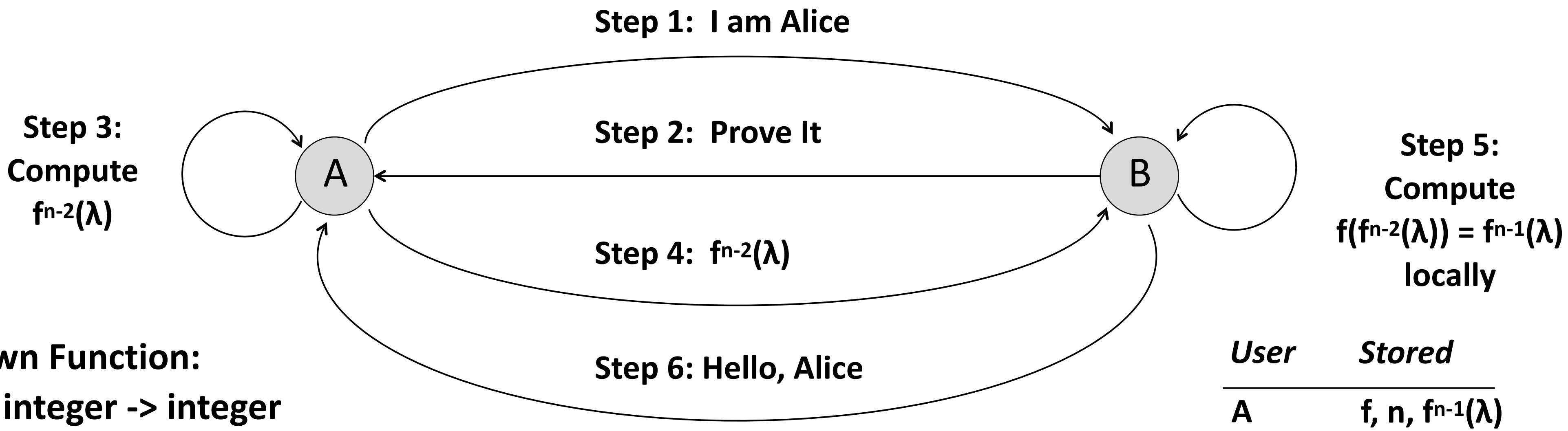
integer λ

Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

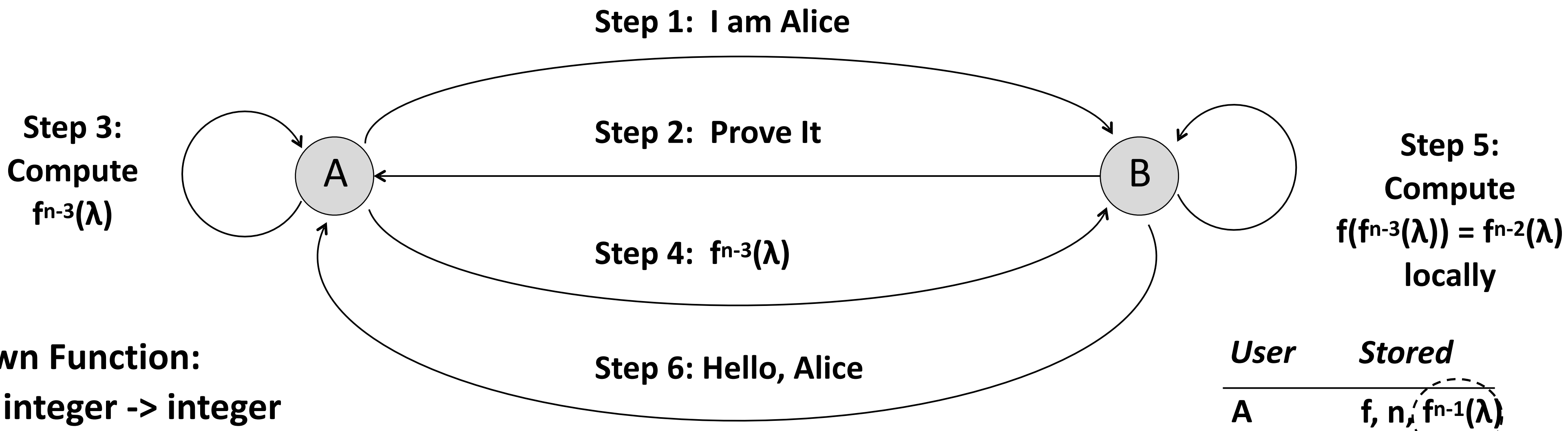
integer λ

Number of Rounds:

n-1 = 9,999

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

Lamport S/Key Protocol



Known Function:

f: integer -> integer

Known Seed:

integer λ

Number of Rounds:

n-1 = 9,998

User	*Stored*
A	**f, n, $f^{n-1}(\lambda)$**

$f^{n-1}(\lambda)$ stored

Lamport S/Key Protocol

A

B

Known Function:

f: integer -> integer

Known Seed:

integer λ

Number of Rounds:

n-2 = 9,998

User	*Stored*
A	**f, n, $f^{n-2}(\lambda)$**

$f^{n-2}(\lambda)$

now stored

(decremented)

Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	-	$f^n(\lambda)$

Week 6

Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	-	$f^n(\lambda)$
Round 2		$f^{n-1}(\lambda)$

Note:
$f(f^{n-1}(\lambda)) = f^n(\lambda)$

Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	$f^{n-1}(\lambda)$	$f^{n}(\lambda)$
Round 2		$f^{n-1}(\lambda)$

Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	$f^{n-1}(\lambda)$	$f^{n}(\lambda)$
Round 2	$f^{n-2}(\lambda)$	$f^{n-1}(\lambda)$
Round 3		$f^{n-2}(\lambda)$

Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	$f^{n-1}(\lambda)$	$f^{n}(\lambda)$
Round 2	$f^{n-2}(\lambda)$	$f^{n-1}(\lambda)$
Round 3	$f^{n-3}(\lambda)$	$f^{n-2}(\lambda)$
Round 4	$f^{n-4}(\lambda)$	$f^{n-3}(\lambda)$

By waiting for successive rounds, observer Eve can see the plaintext for the previous round

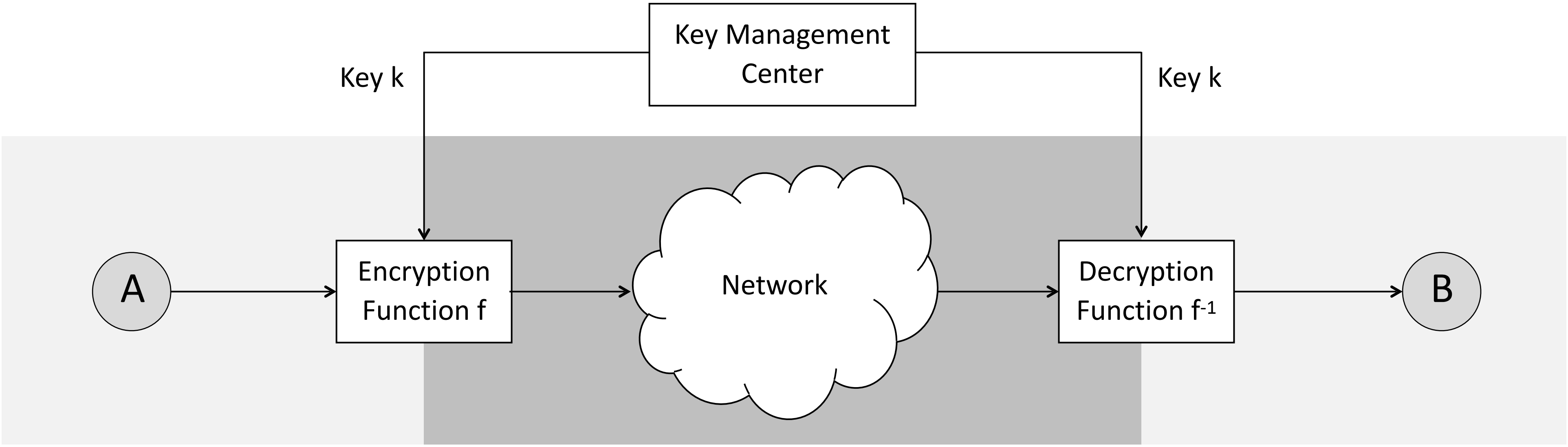
Lamport S/Key Protocol – Analysis

	Input	Output
Round 1	$f^{n-1}(\lambda)$	$f^{n}(\lambda)$
Round 2	$f^{n-2}(\lambda)$	$f^{n-1}(\lambda)$
Round 3	$f^{n-3}(\lambda)$	$f^{n-2}(\lambda)$
Round 4	$f^{n-4}(\lambda)$	$f^{n-3}(\lambda)$

By waiting for successive rounds, observer Eve can see the plaintext for the previous round

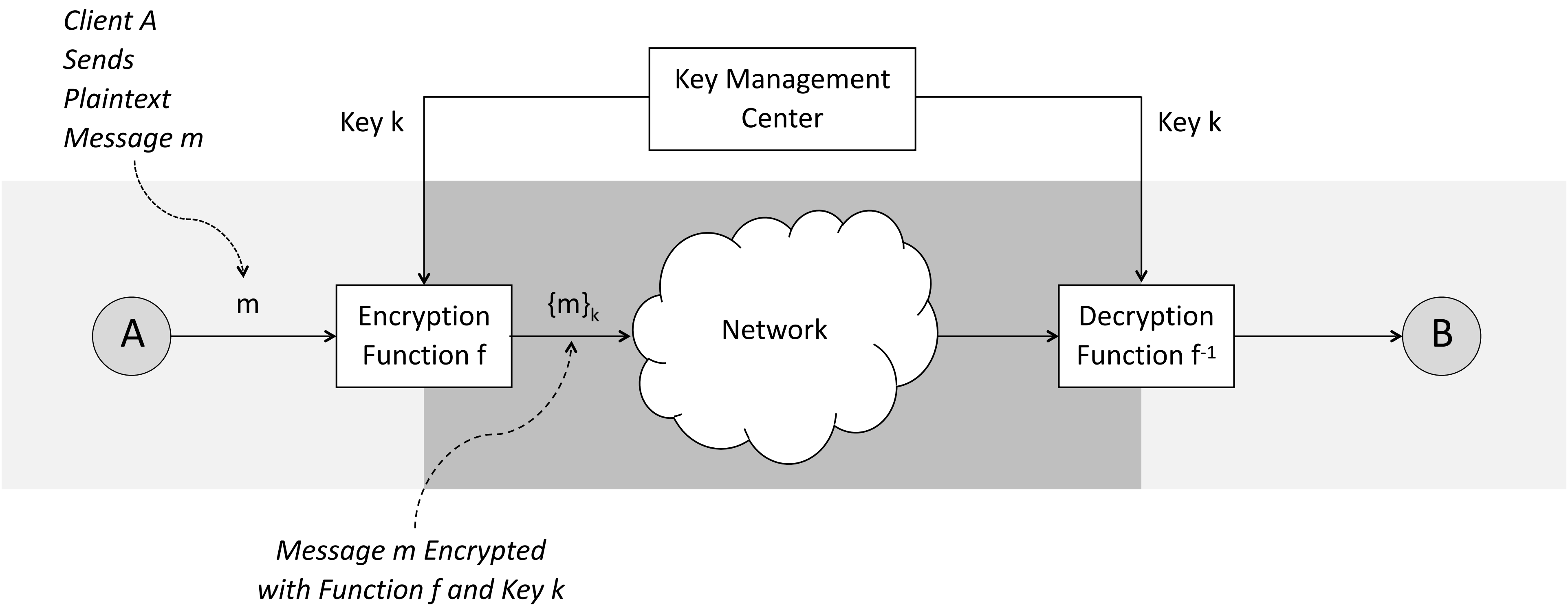
Implies *Known Plaintext* Cryptanalysis

Conventional Encryption Schema



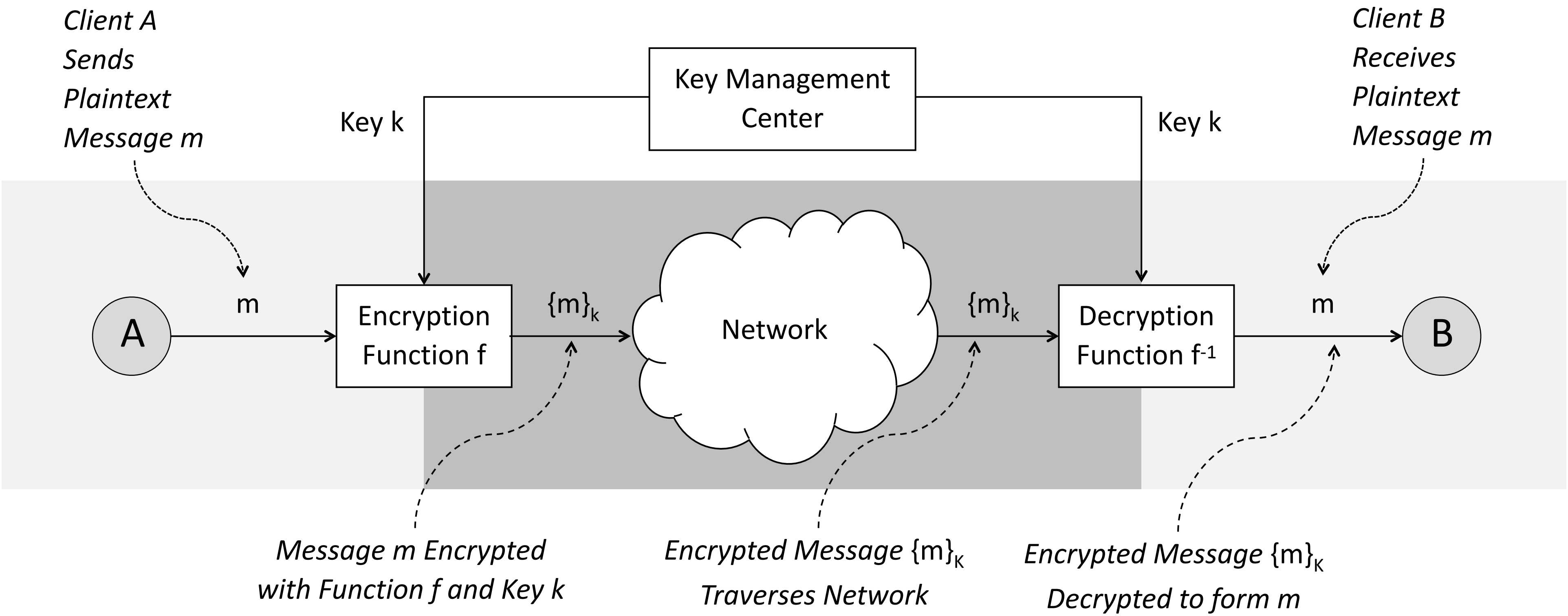
Week 6

Conventional Encryption Schema



Week 6

Conventional Encryption Schema



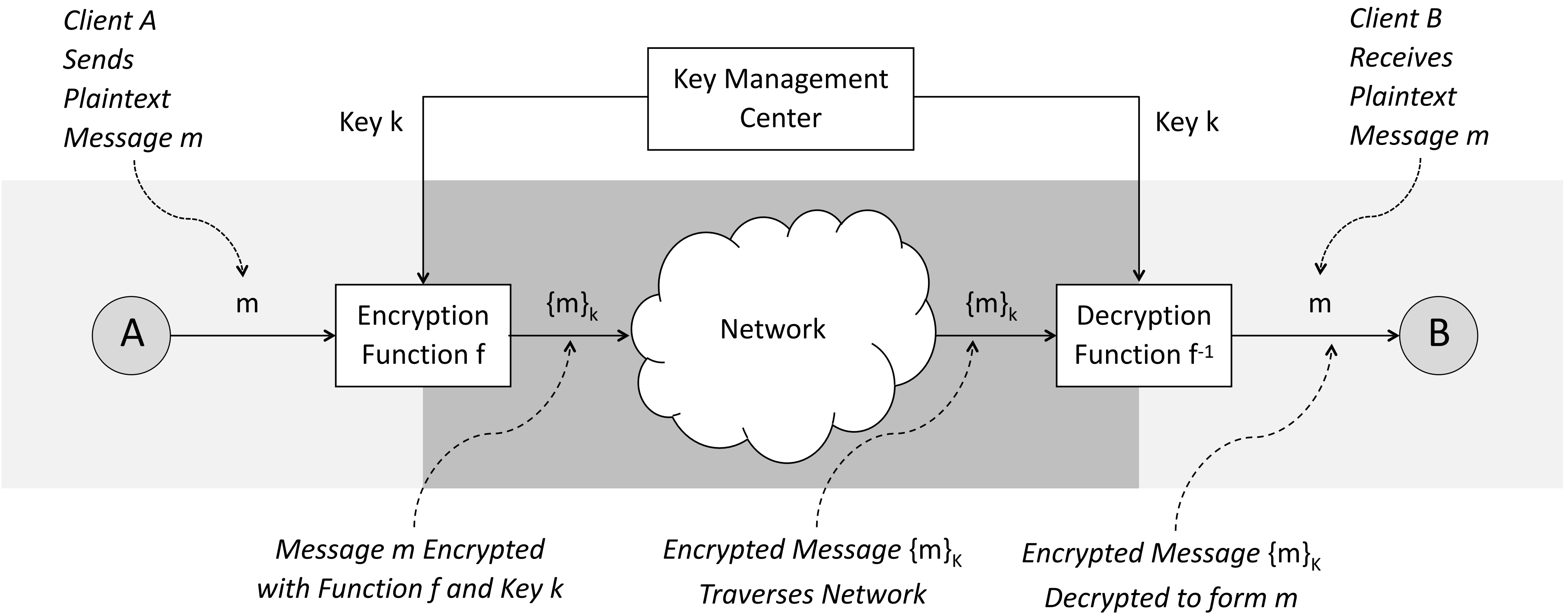
$$\{\,\{m\}_K\,\}_K = m$$

Decrypt with Function f^{-1}

Encrypt with Function f

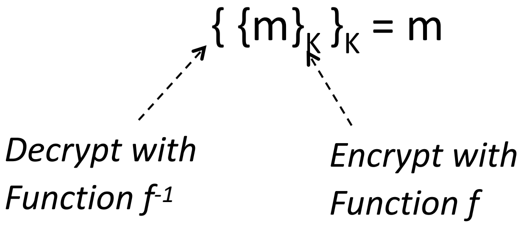
Week 6

Conventional Encryption Schema



Two Important Security Properties:

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



Data Encryption Standard (DES)

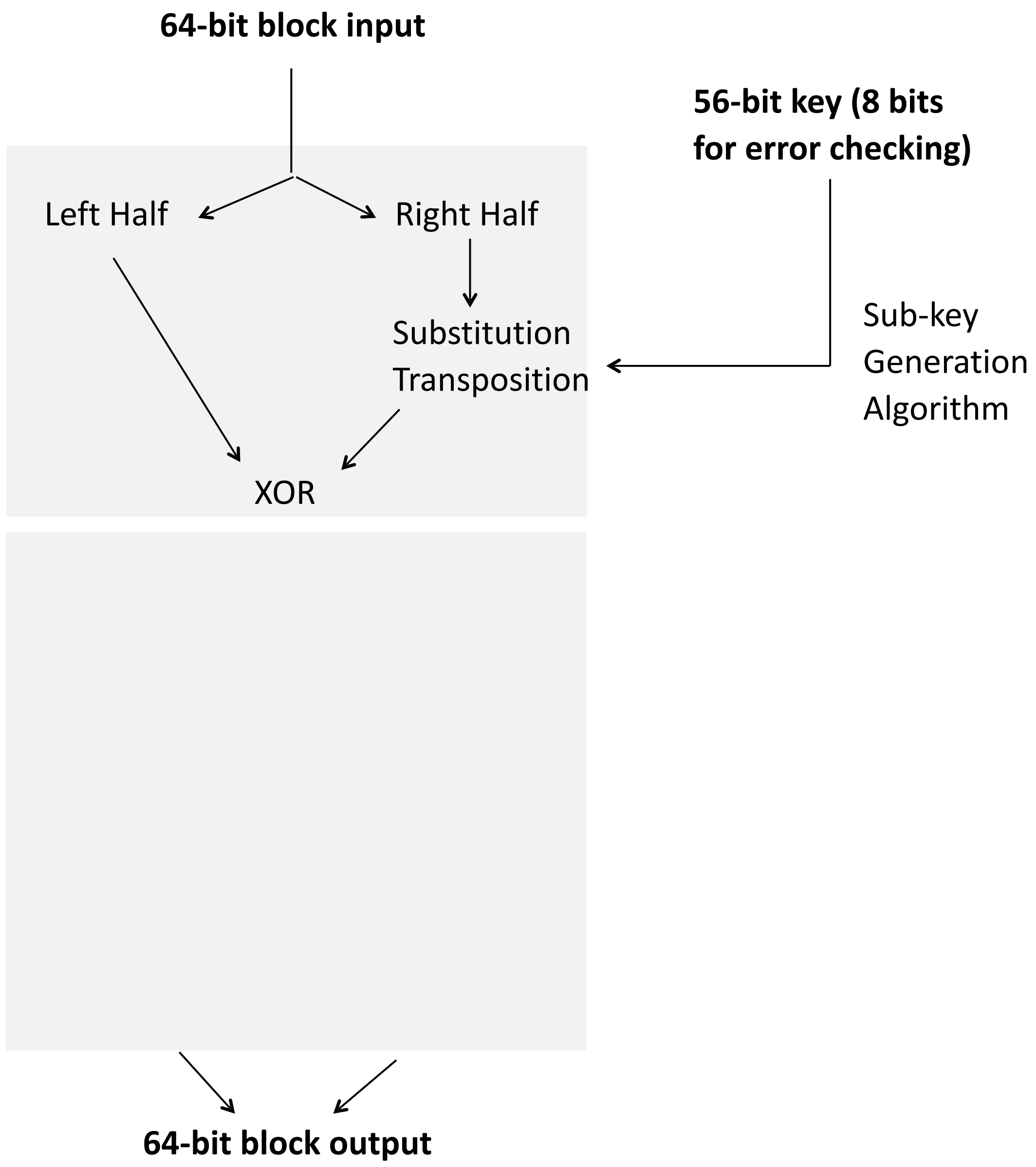
64-bit block input

56-bit key (8 bits for error checking)

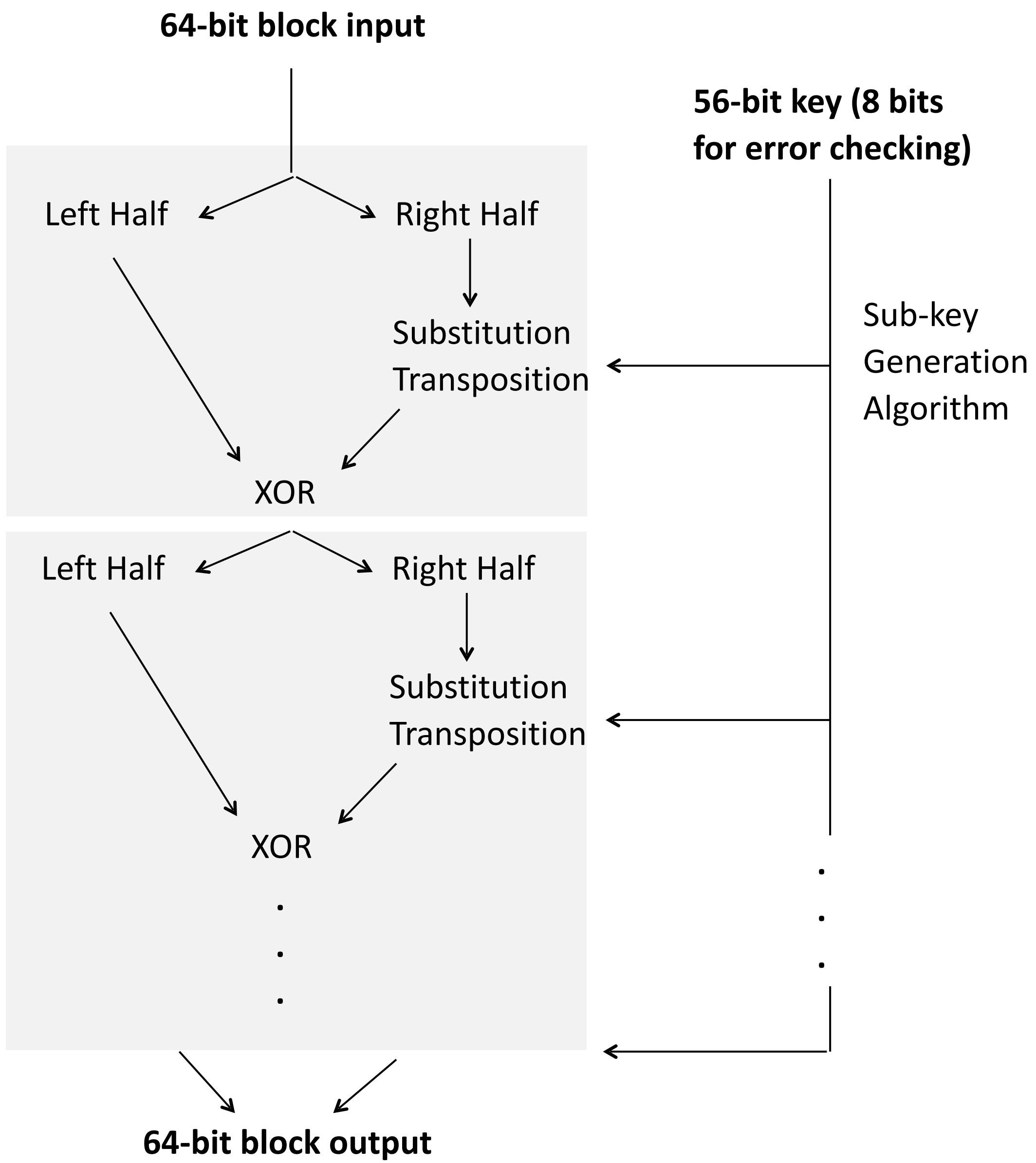
64-bit block output

Week 6

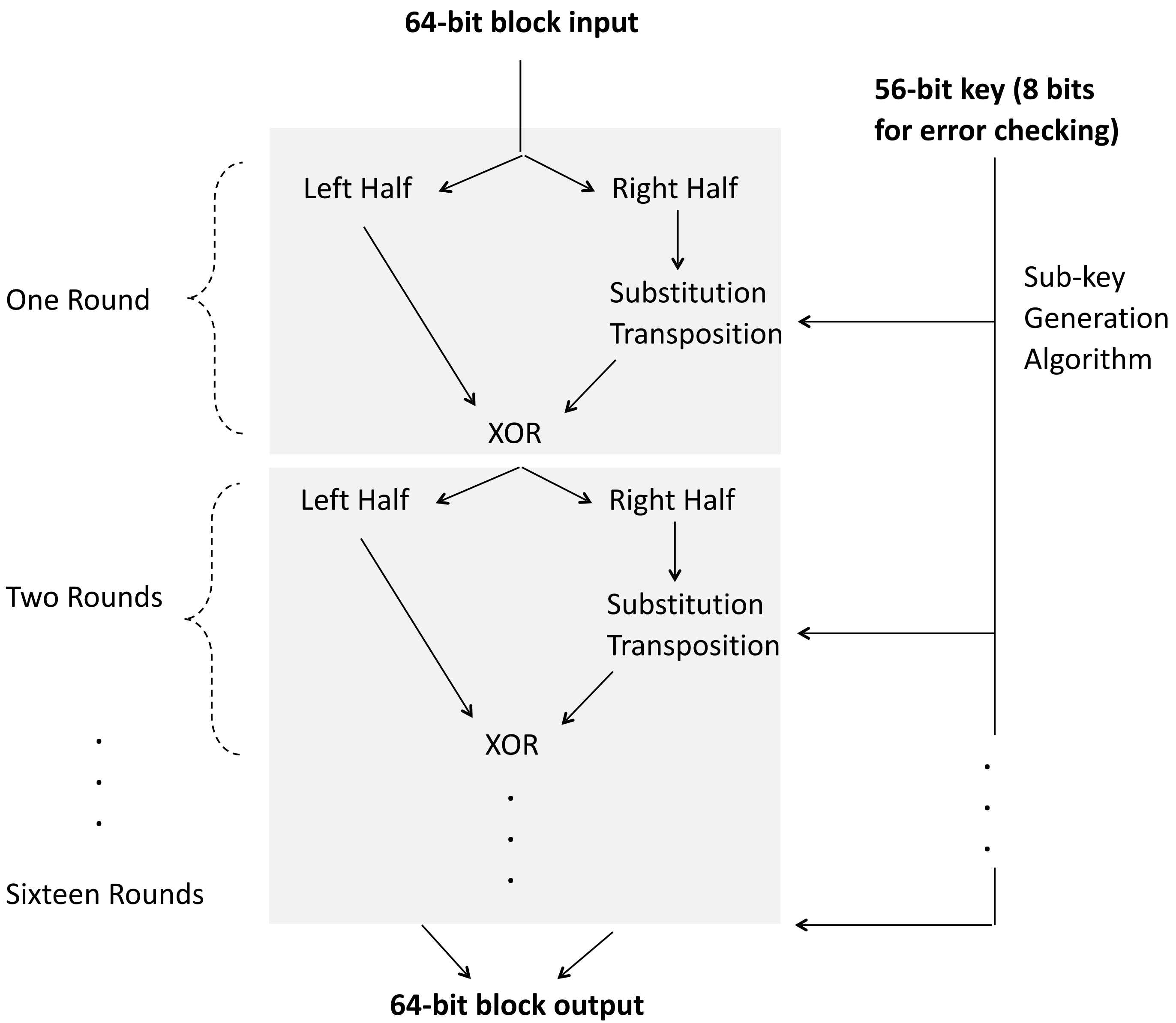
Data Encryption Standard (DES)



Data Encryption Standard (DES)



Data Encryption Standard (DES)



Week 6

Triple-DES

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

Week 6

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: $K1 = K2 \neq K3$

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

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

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

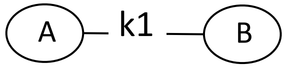
Effective 112 bits

$$\{ \{ \{ m \}_{K1} \}_{K2} \}_{K1}$$

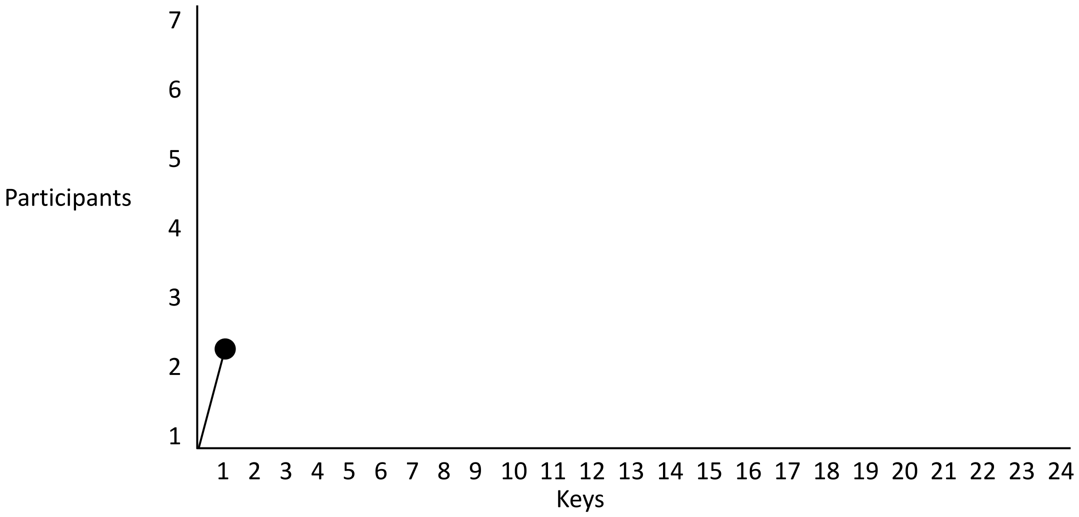
E D E Mode

Week 6

Conventional Encryption Scaling Issue

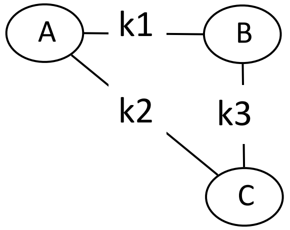


2 participants – 1 shared key



Week 6

Conventional Encryption Scaling Issue

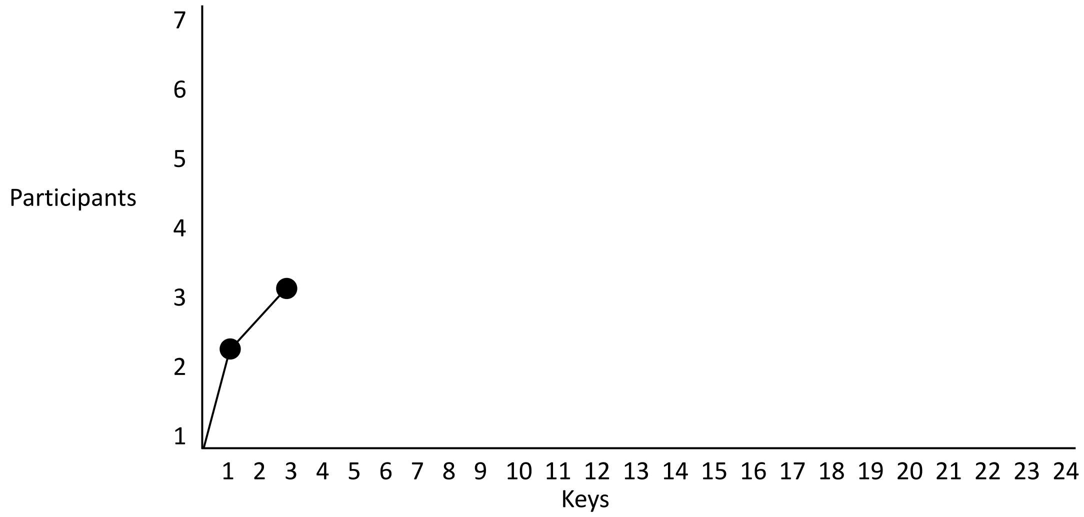


2 participants – 1 shared key

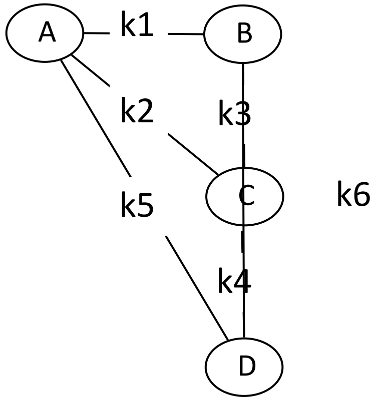
3 participants – 3 shared keys

Added participant 1

Added new keys 2



Conventional Encryption Scaling Issue



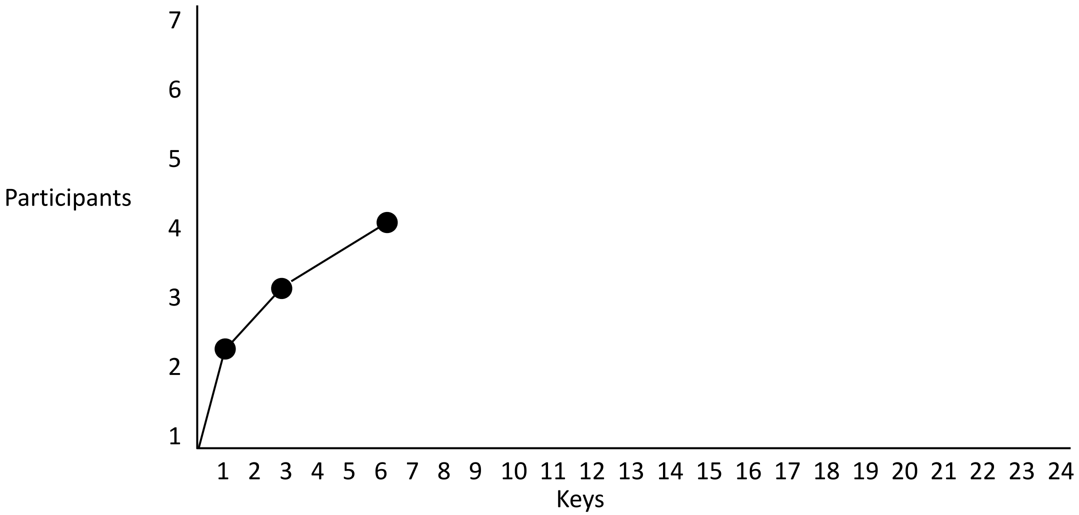
2 participants – 1 shared key

3 participants – 3 shared keys

4 participants – 6 shared keys

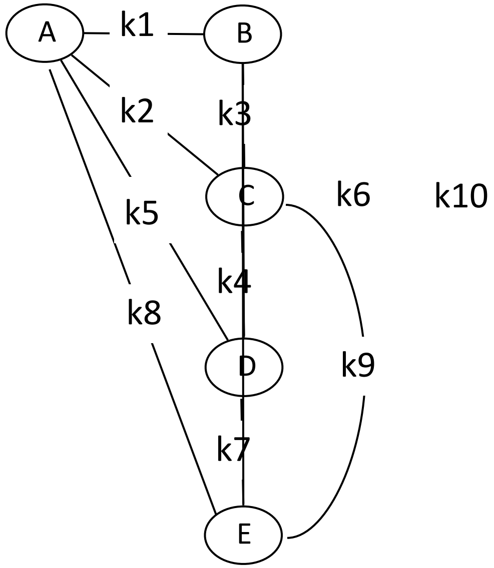
Added participant 1

Added new keys 3



Week 6

Conventional Encryption Scaling Issue

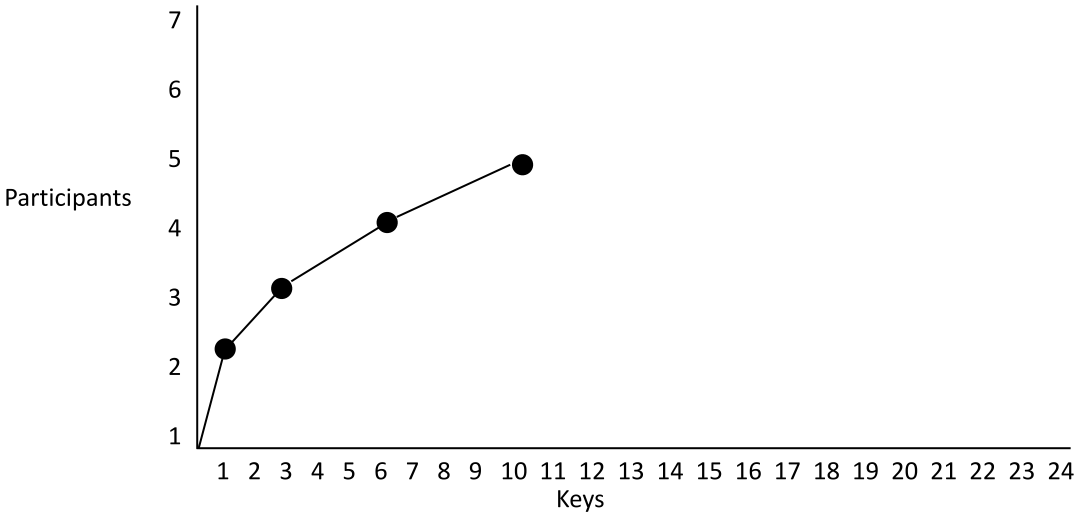


2 participants – 1 shared key

3 participants – 3 shared keys

4 participants – 6 shared keys

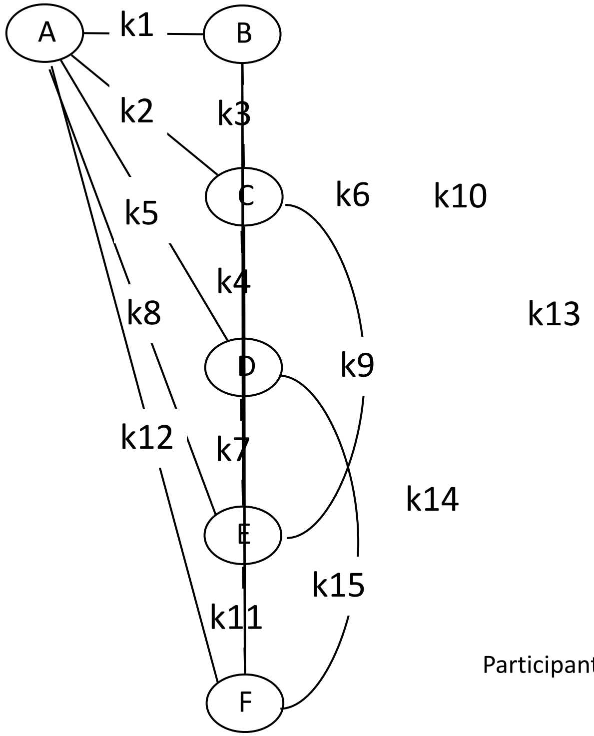
5 participants – 10 shared keys



Added participant 1

Added new keys 4

Conventional Encryption Scaling Issue



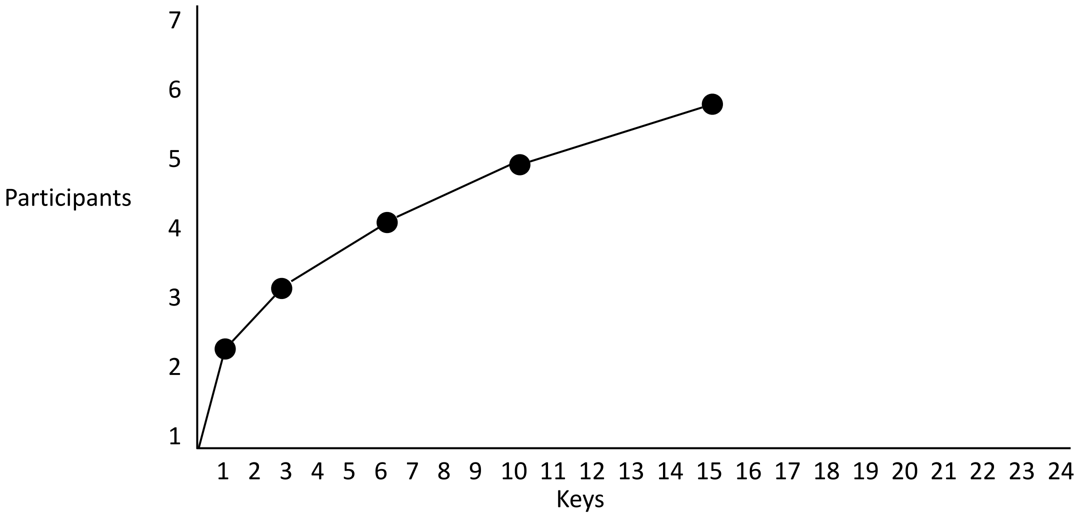
2 participants – 1 shared key

3 participants – 3 shared keys

4 participants – 6 shared keys

5 participants – 10 shared keys

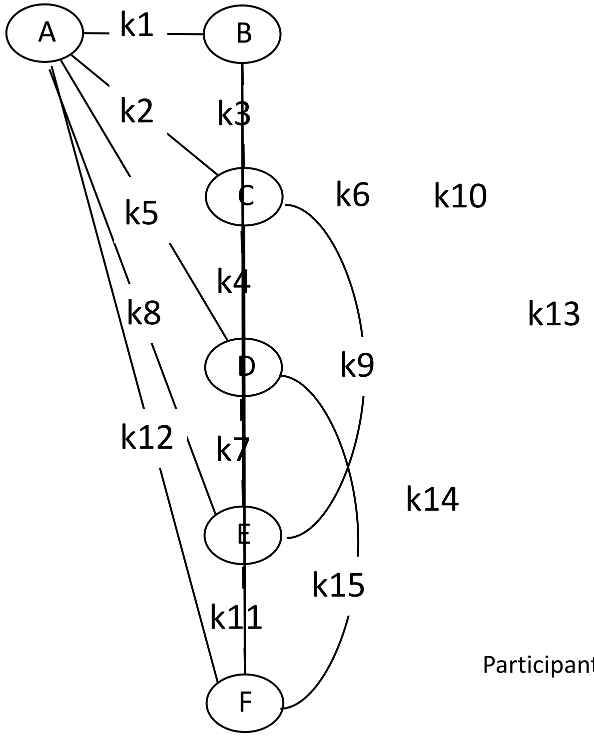
6 participants – 15 shared keys



Added participant 1

Added new keys 5

Conventional Encryption Scaling Issue



2 participants – 1 shared key

3 participants – 3 shared keys

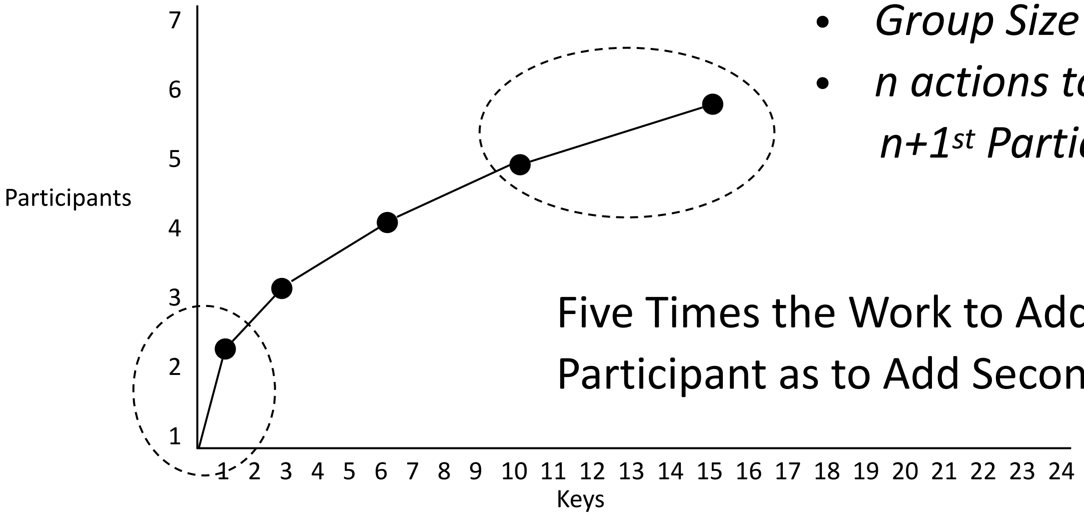
4 participants – 6 shared keys

5 participants – 10 shared keys

6 participants – 15 shared keys

Added participant 1

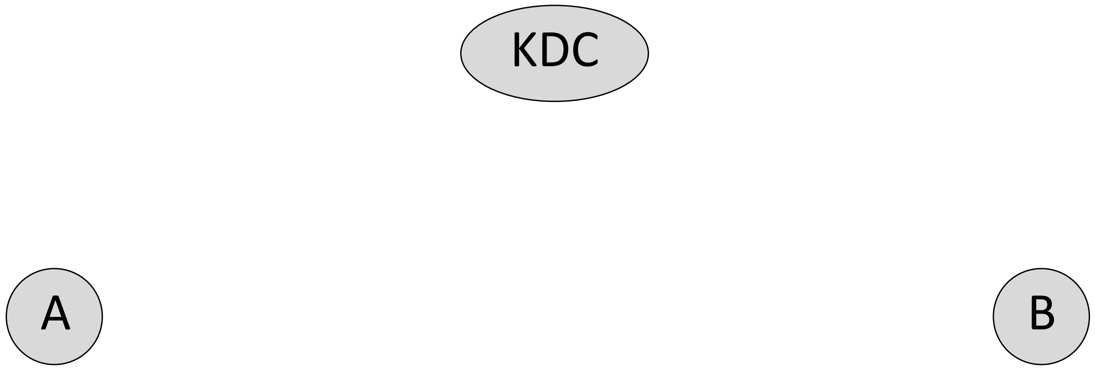
Added new keys 5



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

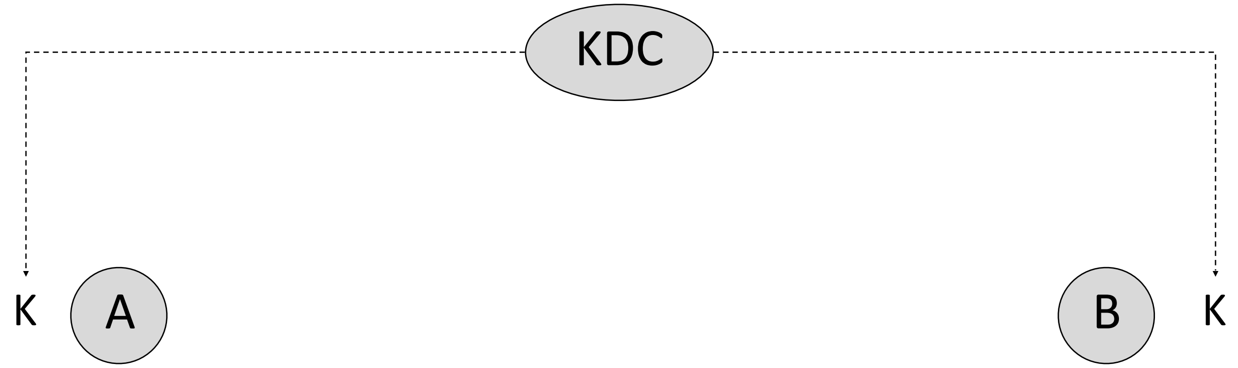
Five Times the Work to Add Sixth Participant as to Add Second

Conventional Cryptography



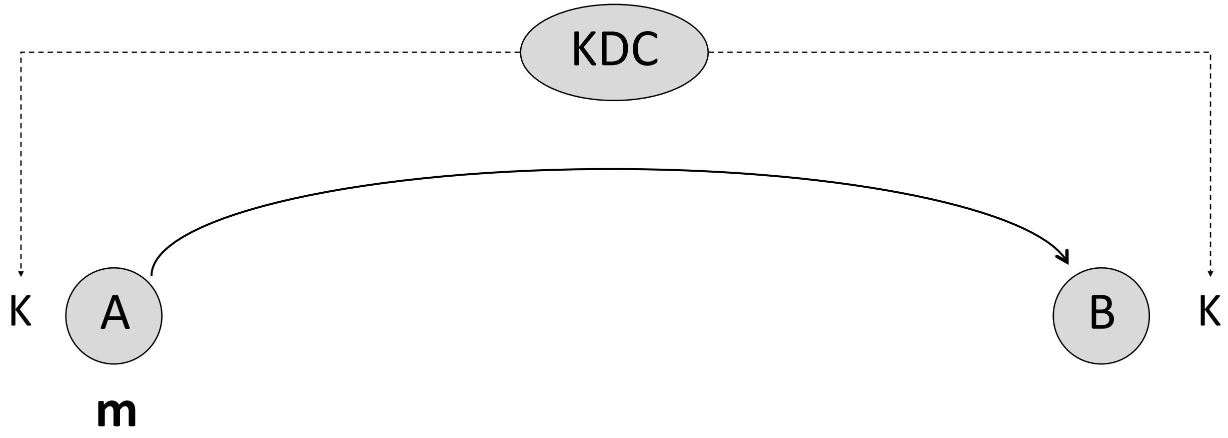
Week 6

Conventional Cryptography



Week 6

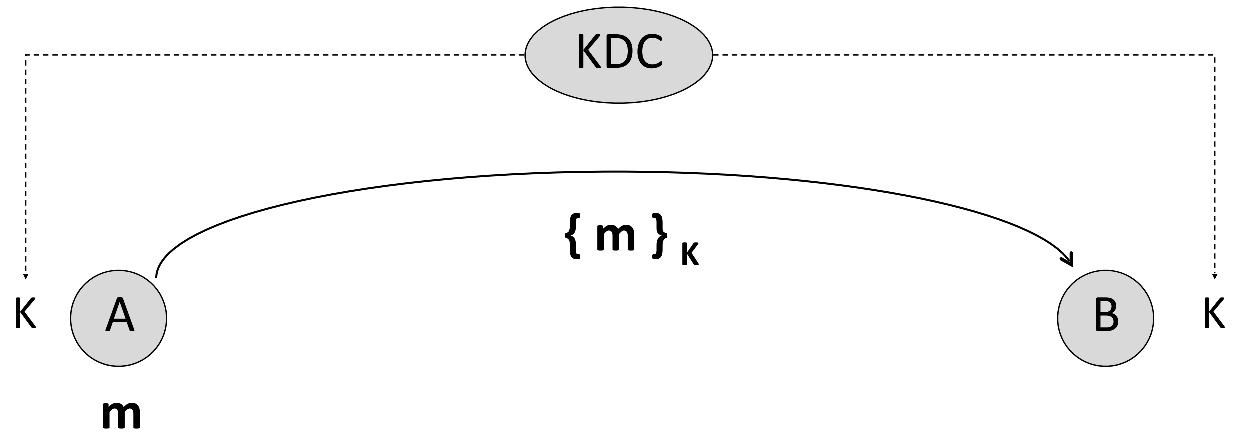
Conventional Cryptography



Alice creates message m . . .

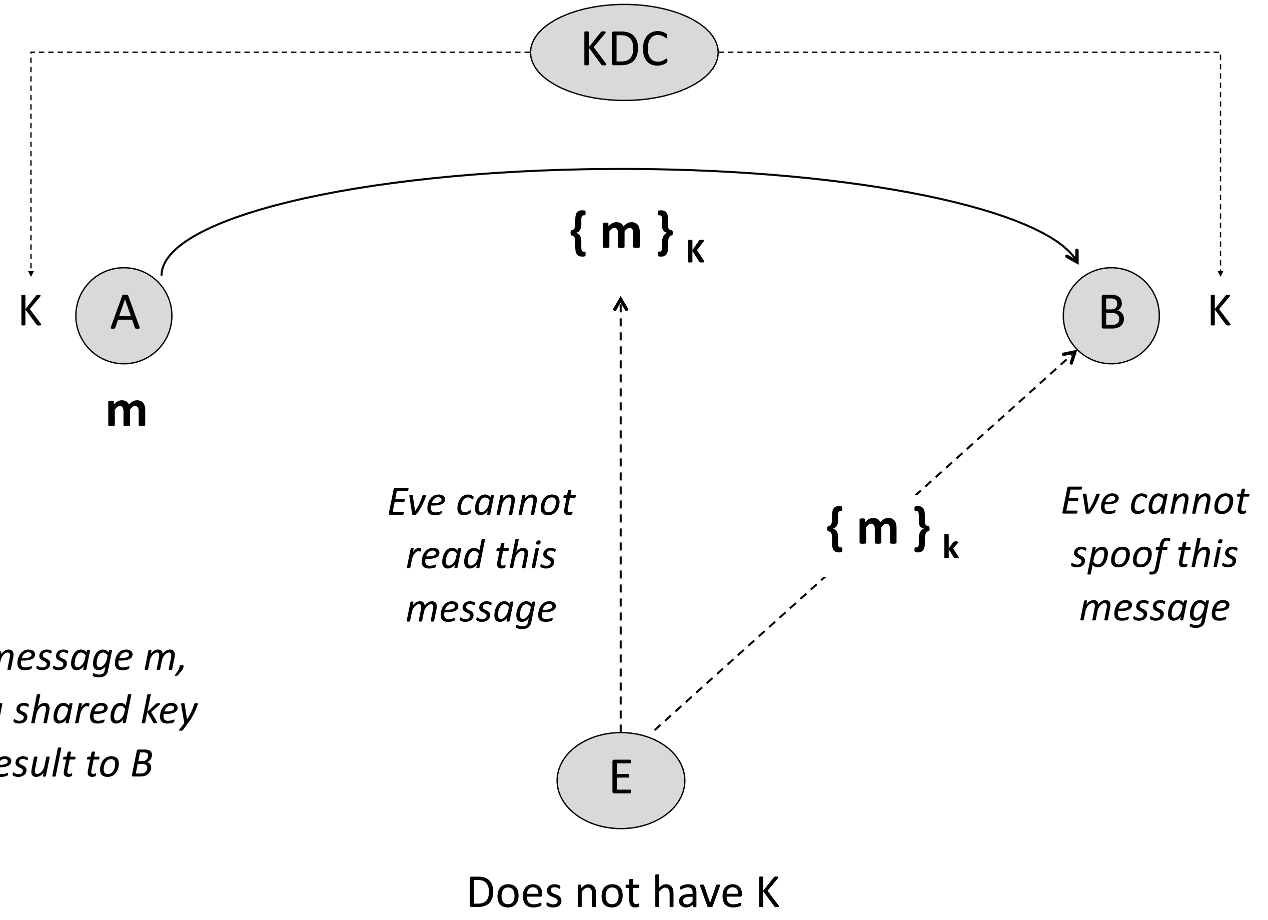
Week 6

Conventional Cryptography



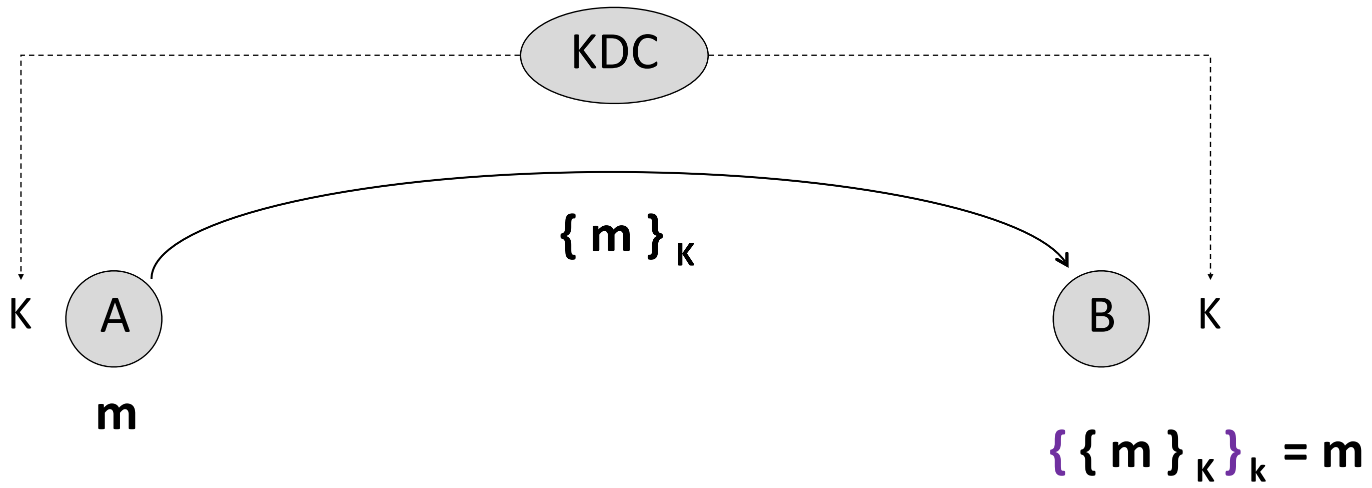
Alice creates message m, encrypts using shared key k, and sends result to B

Conventional Cryptography



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

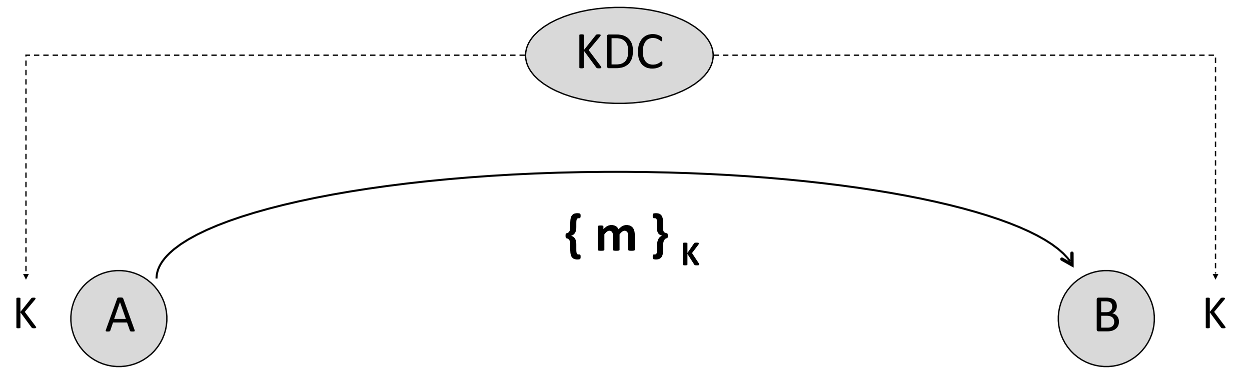
Conventional Cryptography



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

Week 6

Conventional Cryptography

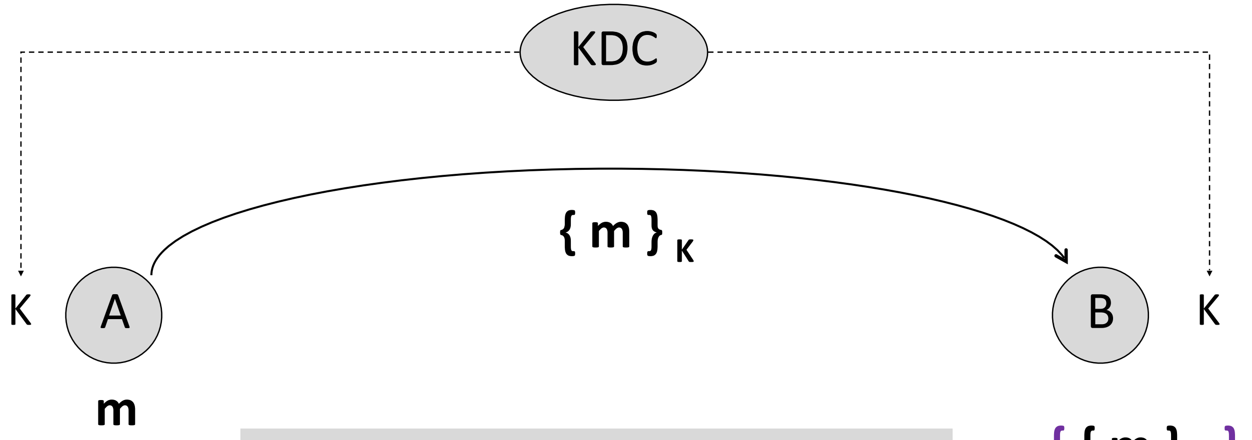


m

$\{\{m\}_K\}_K = m$

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

Conventional Cryptography



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

Secrecy Between A and B? **YES**

Authentication of A by B? **YES**

Does this approach scale? **NO**

Week 6

Conventional Block Cryptography

Stream of "Readable" Data

Plaintext: $\mho_1$ Σ_1 Σ_2 $\mho_2$ $\mho_3$ Σ_3 Σ_4 . . .

Ciphertext: $f(\mho_1)$ $f(\Sigma_1)$ $f(\Sigma_2)$ $f(\mho_2)$ $f(\mho_3)$ $f(\Sigma_3)$ $f(\Sigma_4)$

Presumably No Patterns in Stream of "Unreadable" Block Encrypted Data

Week 6

Conventional Block Cryptography – Covert Channel

Blocks Fixed by Sender into a Pattern

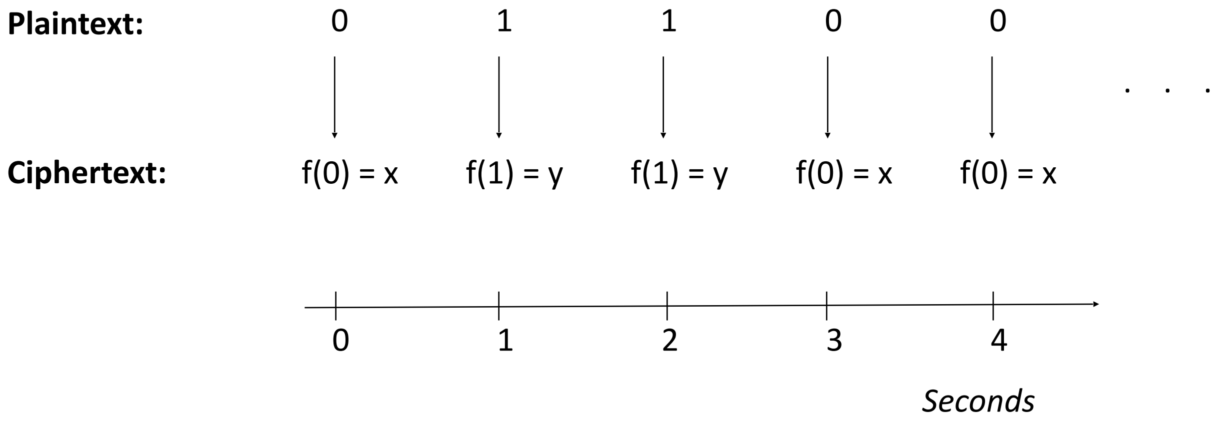
Plaintext: Ʊ Σ Σ Ʊ Ʊ Σ Σ . . .

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

Pattern Can Emerge for External Observer in Encrypted Data

Week 6

Conventional Block Cryptography – 1 bps Channel



Week 6

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)

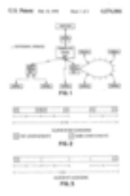
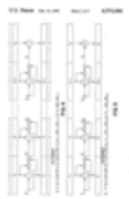
External Links: USPTO, USPTO Assignment, Espacenet

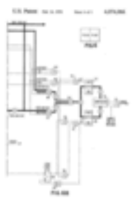
ABSTRACT

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 6

Block Chain Mode Cryptography

Genesis Block

Plaintext: G

$\downarrow$

Ciphertext: $f(G) = c_1$

Week 6

Block Chain Mode Cryptography

Genesis Block

Plaintext: G 1

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

Week 6

Block Chain Mode Cryptography

Genesis Block

Plaintext: G 1 1

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

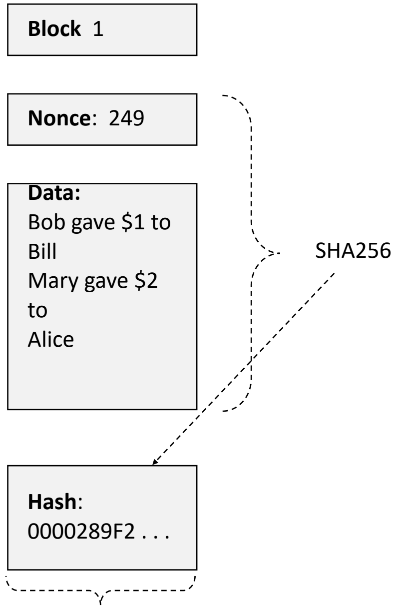
Week 6

Block Chain Mode Cryptography

	Genesis Block				
Plaintext:	G	1	1	0	. . .
	↓	↓	↓	↓	
Ciphertext:	$f(G) = c_1$	$f(c_1, 1)) = c_2$	$f(c_2, 1) = c_3$	$f(c_3, 0) = c_4$	

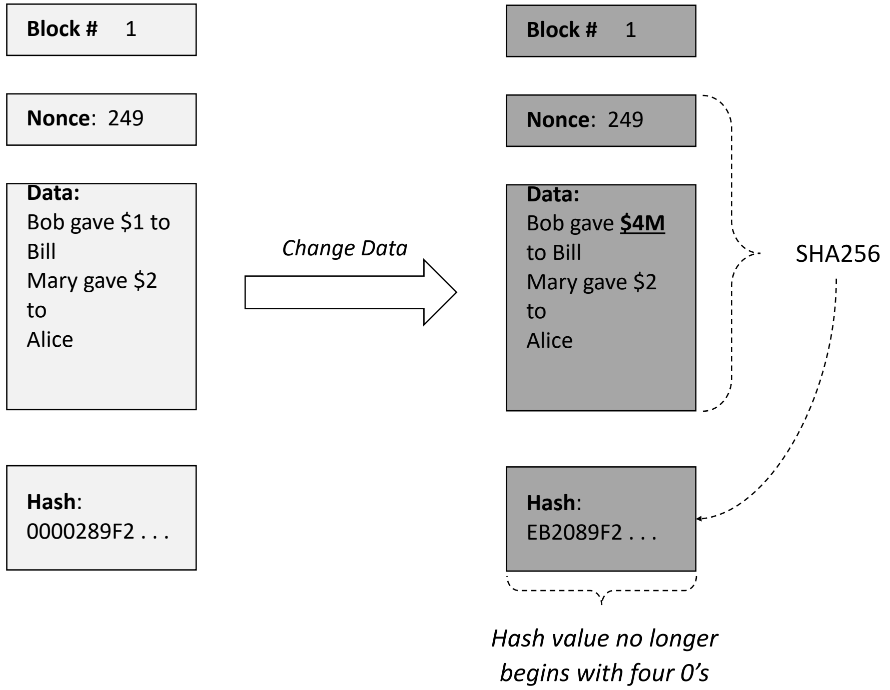
Week 6

Modern Block Chain Usage



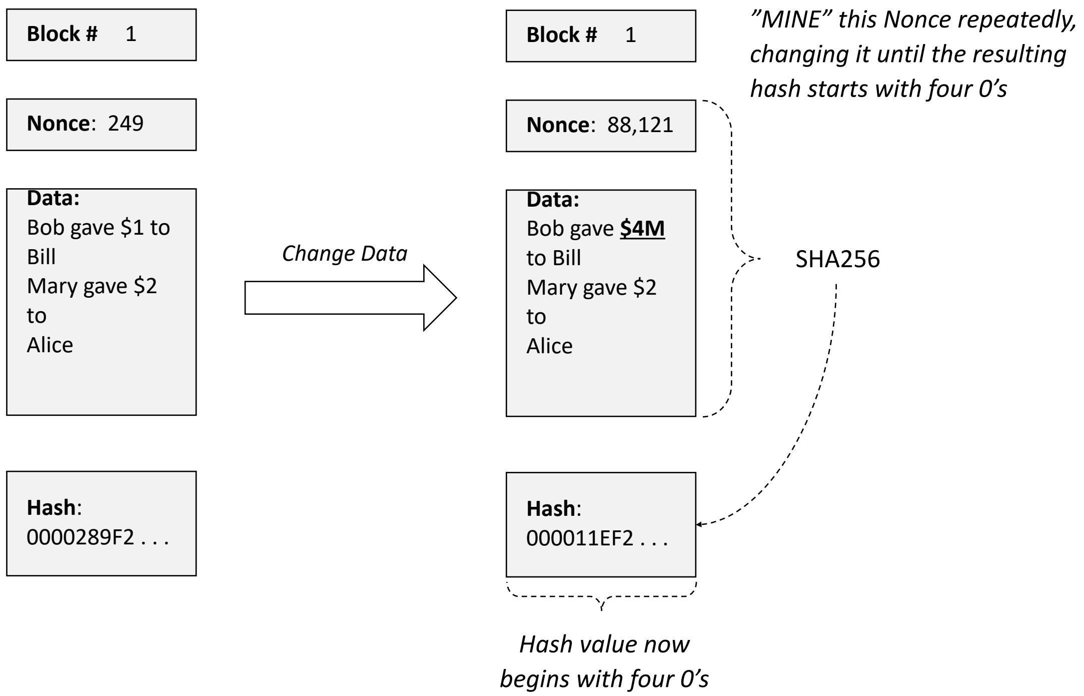
Hash value happens to begin with four 0's

Modern Block Chain Usage



Week 6

Modern Block Chain Usage



Week 6

Modern Block Chain Usage

Block # 1

Nonce: 249

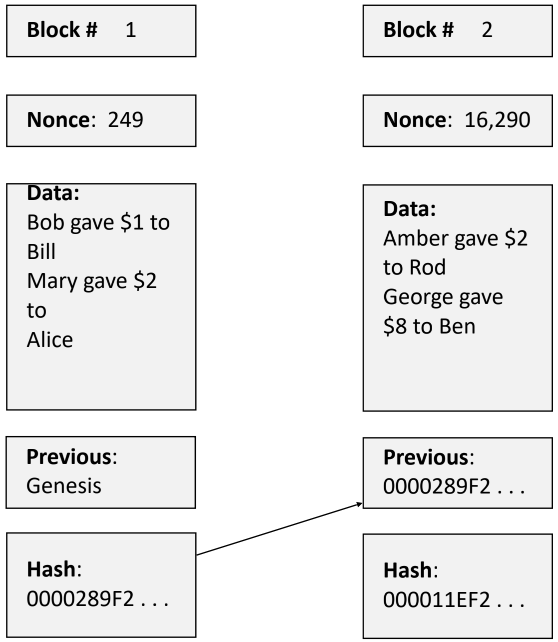
Data:
Bob gave $1 to Bill
Mary gave $2 to Alice

Previous: Genesis

Hash: 0000289F2 . . .

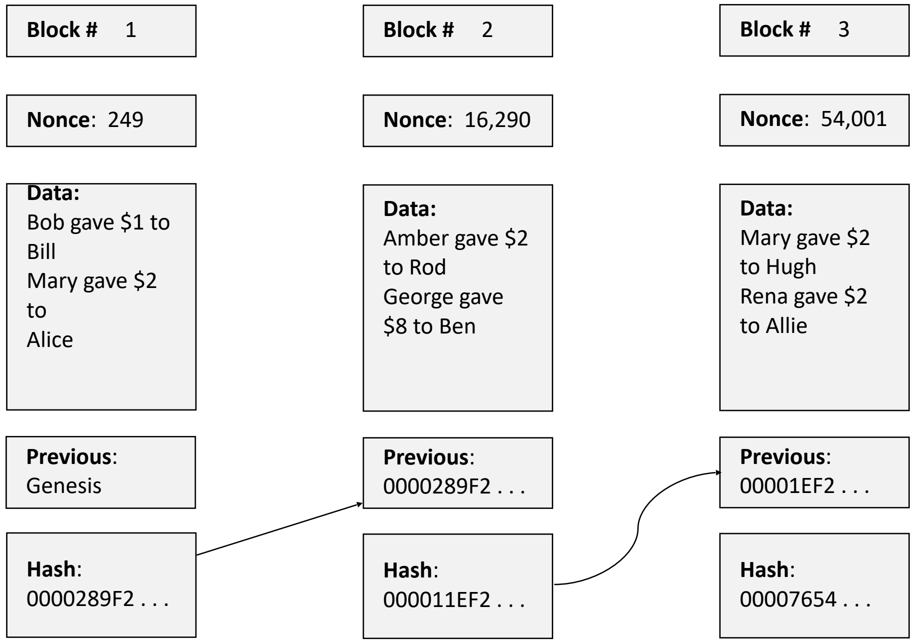
Week 6

Modern Block Chain Usage



Week 6

Modern Block Chain Usage



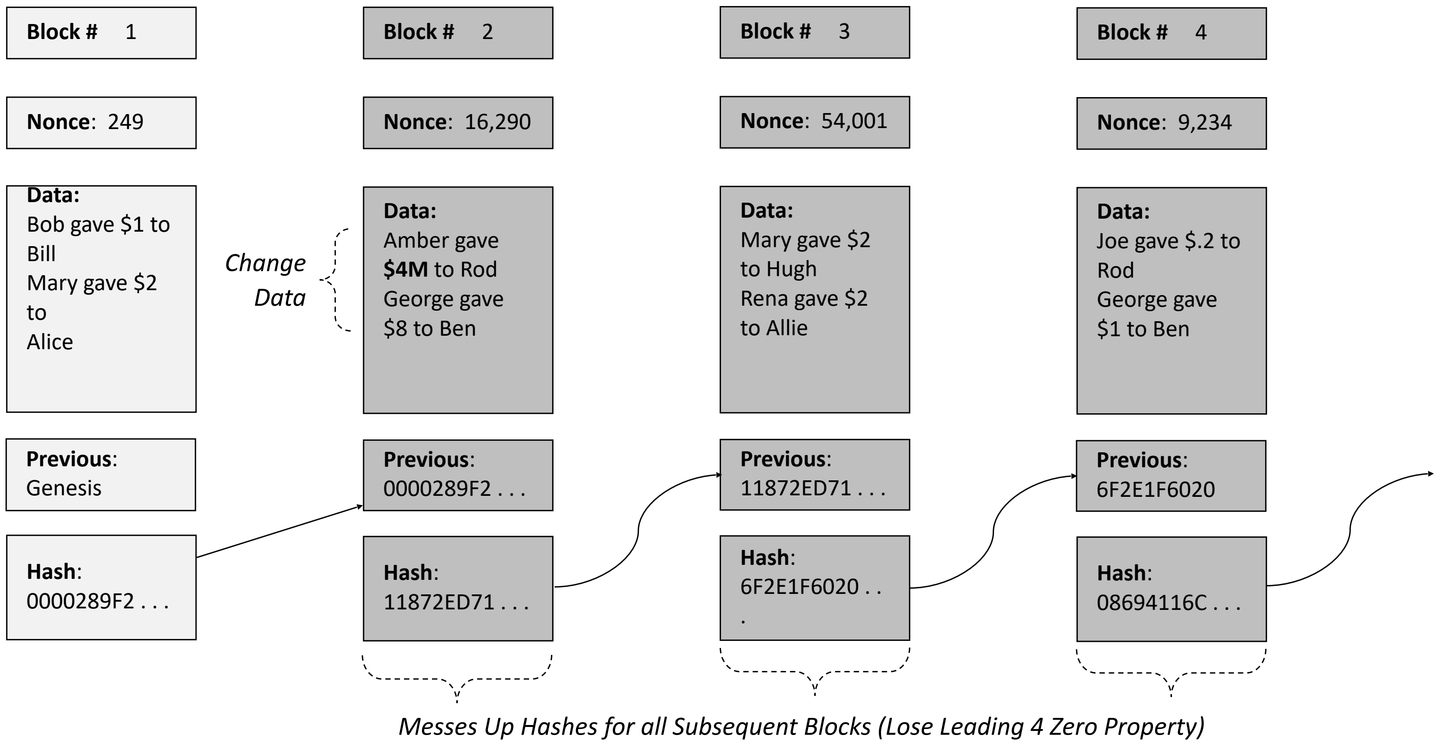
Week 6

Modern Block Chain Usage

Block # 1	**Block #** 2	**Block #** 3	**Block #** 4
Nonce: 249	**Nonce**: 16,290	**Nonce**: 54,001	**Nonce**: 9,234
Data: Bob gave $1 to Bill Mary gave $2 to Alice	**Data:** Amber gave $2 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**: 00001EF2 . . .	**Previous**: 00007654 . . .
Hash: 0000289F2 . . .	**Hash**: 000011EF2 . . .	**Hash**: 00007654 . . .	**Hash**: 0000AA0B . . .

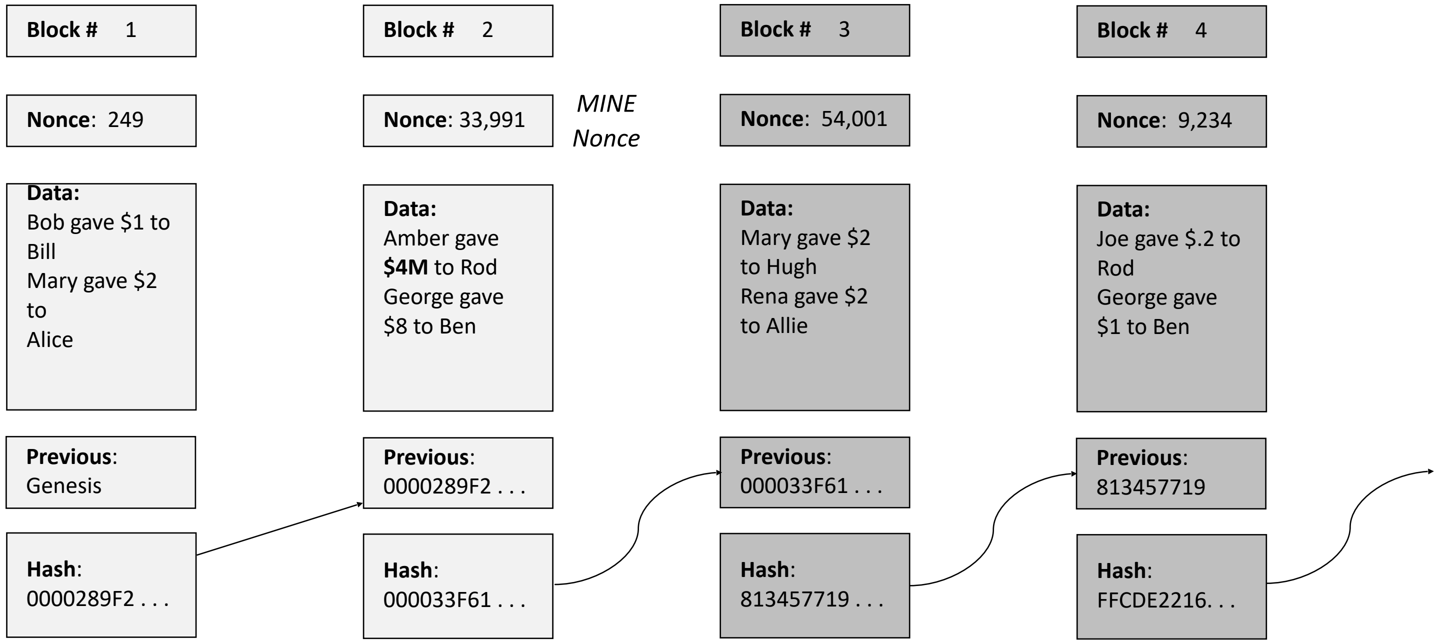
Week 6

Modern Block Chain Usage



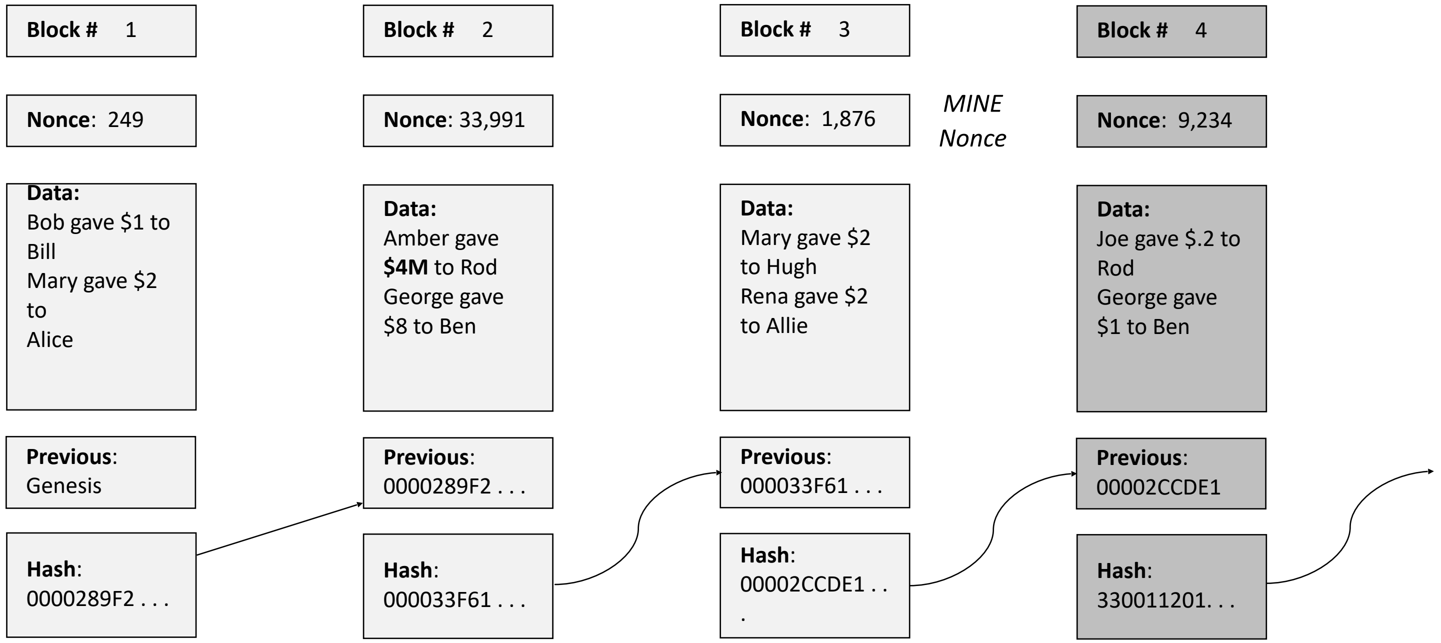
Week 6

Modern Block Chain Usage



Week 6

Modern Block Chain Usage



Week 6

Modern Block Chain Usage

Block # 1	**Block #** 2	**Block #** 3	**Block #** 4	
Nonce: 249	**Nonce**: 33,991	**Nonce**: 1,876	**Nonce**: 128	*MINE Nonce*
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. . .	

Week 6