

Week 3: Block ciphers

Jay Daigle

Occidental College

September 13, 2018

Definition

A block cipher encrypts fixed-sized blocks of ciphertext, rather than single letters at a time.

Permutation cipher

We choose a block size n , and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.

Permutation cipher

We choose a block size n , and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.

To encrypt, we break our plaintext into blocks of size n , padding the final block with nonsense characters if necessary. Then we permute each block according to the key k .

Permutation cipher

We choose a block size n , and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.

To encrypt, we break our plaintext into blocks of size n , padding the final block with nonsense characters if necessary. Then we permute each block according to the key k .

To decrypt, we take the inverse permutation k^{-1} and apply this to each ciphertext block.

“Fourscore and seven years ago”

“Fourscore and seven years ago”

Block size five

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

RFOSU

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

R**F**OSU

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

RF0SU

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

RFOSU

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

R.FOSU

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

fourscore and seven years ago

RFOUS

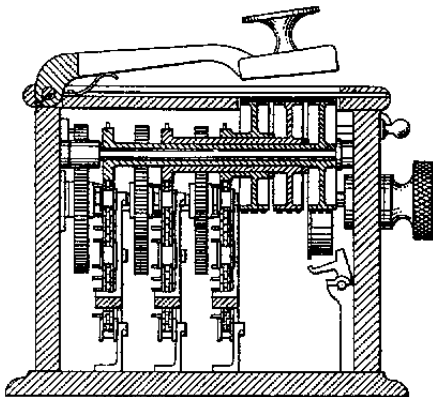
“Fourscore and seven years ago”

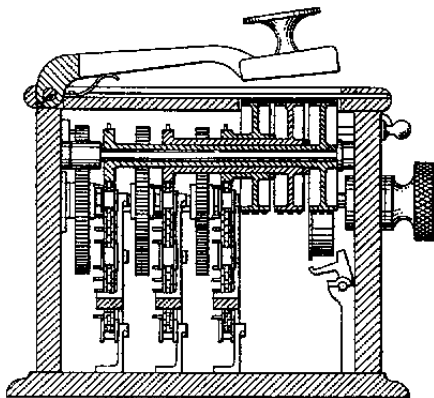
Block size five and key $k = (12345) \mapsto (23514)$.

fours corea ndsev enyea rsago

RFOSU ECOAR ENDVS EENAY GRSOA.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \left(\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$





Lester Hill's patented cipher machine

Hill Cipher

We first choose a block size n . We choose a key, which is a $n \times n$ matrix K with entries in $\mathbb{Z}/26\mathbb{Z}$ (that is, integers modulo 26). We require that $\gcd(26, \det K) = 1$.

We divide our message into blocks of length n . We write each plaintext block as a column vector $B \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext block is given by KB .

To decrypt, we compute K^{-1} in $\mathbb{Z}/26\mathbb{Z}$. Given a ciphertext block C , the corresponding plaintext block is $K^{-1}C$.

“It was a dark and stormy night.”

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

$$K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

$$K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix}$$

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix}$$

$$K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

$$K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix}$$

$$K \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

“It was a dark and stormy night.”

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

$$K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix}$$

$$K \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

RA OG CM JP JA NA BZ TT LF HQ EA OV

how are you today

how are you today

ZWS ENI USP LJVEU

how are you today

ZWS ENI USP LJVEU

07-14 22-00 17-04 24-14 20-19 14-03 00-24

how are you today

ZWS ENI USP LJVEU

07-14 22-00 17-04 24-14 20-19 14-03 00-24

25-22 18-08 13-08 20-18 15-11 09-21 04-20



Claude Shannon

Picture CC BY-SA 2.0 de by Konrad Jacobs

Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

Definition

An encryption method has good confusion if the key does not relate straightforwardly to the ciphertext, but each part of the ciphertext depends on many parts of the key.