UC SANTA CRUZ

Math 134: Cryptography

Lecture 15: Block ciphers

Eoin Mackall

February 12, 2025

University of California, Santa Cruz

Encryption so far

Encryption so far

So far we've seen the following cryptosystems:

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers
    1.2 Affine ciphers

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers
    1.2 Affine ciphers
    1.3 Substitution ciphers

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers
    1.2 Affine ciphers
    1.3 Substitution ciphers
2. Public (asymmetric) key

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers
    1.2 Affine ciphers
    1.3 Substitution ciphers
2. Public (asymmetric) key
    2.1 RSA

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
    1.1 Shift ciphers
    1.2 Affine ciphers
    1.3 Substitution ciphers
2. Public (asymmetric) key
    2.1 RSA
    2.2 ElGamal

Encryption so far

So far we've seen the following cryptosystems:

1. Private (symmetric) key
   - 1.1 Shift ciphers
   - 1.2 Affine ciphers
   - 1.3 Substitution ciphers
2. Public (asymmetric) key
   - 2.1 RSA
   - 2.2 ElGamal

Question

What benefits do RSA and ElGamal have over the classical ciphers?

Table of contents

Diffusion and Confusion

Diffusion

Claude Shannon[1] proposed two properties that a good cryptosystem must have:

[1] *Communication theory of secrecy systems.* Bell Systems Technical Journal, **28** (1949), 656–715

Diffusion

Claude Shannon[1] proposed two properties that a good cryptosystem must have:

Diffusion

[1] *Communication theory of secrecy systems.* Bell Systems Technical Journal, **28** (1949), 656–715

Diffusion

Claude Shannon[1] proposed two properties that a good cryptosystem must have:

Diffusion

A good cipher should be strongly diffuse:

[1] *Communication theory of secrecy systems.* Bell Systems Technical Journal, **28** (1949), 656–715

Diffusion

Claude Shannon[1] proposed two properties that a good cryptosystem must have:

Diffusion

A good cipher should be strongly diffuse:

1. small changes in the plaintext should correspond to potentially substantial changes in the ciphertext;

[1] *Communication theory of secrecy systems.* Bell Systems Technical Journal, **28** (1949), 656–715

Diffusion

Claude Shannon[1] proposed two properties that a good cryptosystem must have:

Diffusion

A good cipher should be strongly diffuse:

1. small changes in the plaintext should correspond to potentially substantial changes in the ciphertext;
2. and small changes in the ciphertext should correspond to potentially substantial changes in the plaintext.

[1] *Communication theory of secrecy systems.* Bell Systems Technical Journal, **28** (1949), 656–715

Diffusion

Example (RSA)

Using the public key $(n, e) = (108733, 3)$ the plaintext message

`The cat sings`

is transformed into the ciphertext

`79065 98646 62594 97970 6922 76136 27`.

Diffusion

Example (RSA)

Using the public key $(n, e) = (108733, 3)$ the plaintext message

`The cat sings`

is transformed into the ciphertext

`79065 98646 62594 97970 6922 76136 27`.

The plaintext message

`The bat sings`

is transformed to the ciphertext

`79065 98646 9956 100280 17509 22590 343`.

Diffusion

Nonexample (Affine ciphers)

Using the key $(\alpha, \beta) = (11, 15)$ the plaintext message

`The cat sings`

is transformed into the ciphertext

`Qoh lpq fzcdf`.

Diffusion

Nonexample (Affine ciphers)

Using the key $(\alpha, \beta) = (11, 15)$ the plaintext message

`The cat sings`

is transformed into the ciphertext

`Qoh lpq fzcdf`.

The plaintext message

`The bat sings`

is transformed to the ciphertext

`Qoh  apq fzcdf`.

Confusion

The other property proposed by Shannon is:

Confusion

The other property proposed by Shannon is:

Confusion

Confusion

The other property proposed by Shannon is:

Confusion

A good cipher should “hide the key” among the ciphertext.

Confusion

The other property proposed by Shannon is:

Confusion

A good cipher should “hide the key” among the ciphertext.

In particular, each character of the ciphertext should depend on several parts of the key.

Confusion

The other property proposed by Shannon is:

Confusion

A good cipher should “hide the key” among the ciphertext.

In particular, each character of the ciphertext should depend on several parts of the key.

Remark

This property makes it difficult to find the key from the ciphertext.

If a single bit in a key is changed, then the calculation of most or all of the bits in the ciphertext will be affected.

Confusion

Example (RSA)

Using the public key $(n, e) = (108733, 3)$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`79065 98646 62594 97970 6922 76136 27`.

Confusion

Example (RSA)

Using the public key $(n, e) = (108733, 3)$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`79065 98646 62594 97970 6922 76136 27`.

Using the public key $(n, e) = (109691, 3)$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`51283 68469 65468 14624 39494 99607 27`.

Confusion

Example (RSA)

Using the public key $(n, e) = (108733, 3)$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`79065 98646 62594 97970 6922 76136 27`.

Using the public key $(n, e) = (109691, 3)$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`51283 68469 65468 14624 39494 99607 27`.

Confusion

Example (Shift ciphers)

Using the key $k = 3$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`Wkh fdw vlqjv`.

Confusion

Example (Shift ciphers)

Using the key $k = 3$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`Wkh fdw vlqjv`.

Using the key $k = 4$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`Xli gex wmrkw`.

Confusion

Example (Shift ciphers)

Using the key $k = 3$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`Wkh fdw vlqjv`.

Using the key $k = 4$, the plaintext message

`The cat sings`

is transformed into the ciphertext

`Xli gex wmrkw`.

Block ciphers

Block ciphers

In the classical ciphers (e.g. shift, affine, substitution), we change one letter of plaintext at a time using the given key.

Block ciphers

In the classical ciphers (e.g. shift, affine, substitution), we change one letter of plaintext at a time using the given key.

In a *block cipher*, we change blocks of plaintext characters at a time. Each character in the block should contribute to the ciphertext.

Block ciphers

In the classical ciphers (e.g. shift, affine, substitution), we change one letter of plaintext at a time using the given key.

In a *block cipher*, we change blocks of plaintext characters at a time. Each character in the block should contribute to the ciphertext.

Example

RSA and ElGamal are both examples of block ciphers.

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Suppose that Alice and Bob want to set up a channel for encrypted communication. How will they do this?

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Suppose that Alice and Bob want to set up a channel for encrypted communication. How will they do this?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Suppose that Alice and Bob want to set up a channel for encrypted communication. How will they do this?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

2. Alice and Bob will agree beforehand on a secret (private) $n \times n$-matrix M with $\gcd(\det(M), 26) = 1$ for some integer $n \geq 2$.

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Suppose that Alice and Bob want to set up a channel for encrypted communication. How will they do this?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

2. Alice and Bob will agree beforehand on a secret (private) $n \times n$-matrix M with $\gcd(\det(M), 26) = 1$ for some integer $n \geq 2$.
3. To send a message m, the plaintext is broken into blocks of size n, say $m_1, m_2, \ldots$.

Hill ciphers (encryption)

The (seemingly) earliest example of a block cipher is the Hill cipher.

Suppose that Alice and Bob want to set up a channel for encrypted communication. How will they do this?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

2. Alice and Bob will agree beforehand on a secret (private) $n \times n$-matrix M with $\gcd(\det(M), 26) = 1$ for some integer $n \geq 2$.
3. To send a message m, the plaintext is broken into blocks of size n, say $m_1, m_2, \ldots$.
4. The sender will send the ciphertext blocks $M \cdot m_i$.

Example

Example

Alice wants to send Bob the message `The cat sings`. Bob and Alice have agreed to use the following matrix

$$M = \begin{pmatrix} 11 & 2 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix}$$

with determinant $\det(M) \equiv 7 \pmod{26}$.

Example

Example

Alice wants to send Bob the message `The cat sings`. Bob and Alice have agreed to use the following matrix

$$M = \begin{pmatrix} 11 & 2 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix}$$

with determinant $\det(M) \equiv 7 \pmod{26}$.

Alice breaks her message up to submessages, the first being $m_1 = (T, h, e)^\top = (19, 7, 4)^\top$. She calculates

$$M \cdot m_1 = \begin{pmatrix} 11 & 2 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 19 \\ 4 \end{pmatrix} \pmod{26}.$$

And sends the corresponding ciphertext `Bte`.

Hill ciphers (decryption)

If Bob receives a message from Alice (or vice-versa), how will he (or she) decrypt it?

Hill ciphers (decryption)

If Bob receives a message from Alice (or vice-versa), how will he (or she) decrypt it?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

Hill ciphers (decryption)

If Bob receives a message from Alice (or vice-versa), how will he (or she) decrypt it?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

2. The message receiver will calculate an inverse M^{-1} modulo 26, which is possible since $\gcd(\det(M), 26) = 1$.

Hill ciphers (decryption)

If Bob receives a message from Alice (or vice-versa), how will he (or she) decrypt it?

1. Like in the classical ciphers, Alice and Bob will use the following conversion for their plaintext characters.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25

2. The message receiver will calculate an inverse M^{-1} modulo 26, which is possible since $\gcd(\det(M), 26) = 1$.
3. If the ciphertext received is $c_1 = M \cdot m_1, c_2 = M \cdot m_2, c_3 = M \cdot m_3, \ldots$, then the plaintext is obtained by calculating

$$M^{-1}c_i \equiv M^{-1}(Mm_i) \equiv (M^{-1}M)m_i \equiv m_i \pmod{26}.$$

Example

Example

Alice has sent Bob the message `Bte...`. Bob and Alice have agreed to use the following matrix

$$M = \begin{pmatrix} 11 & 2 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix}$$

with determinant $\det(M) \equiv 7 \pmod{26}$.

Example

Example

Alice has sent Bob the message `Bte...`. Bob and Alice have agreed to use the following matrix

$$M = \begin{pmatrix} 11 & 2 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix}$$

with determinant $\det(M) \equiv 7 \pmod{26}$.

Bob finds an inverse of M, say M^{-1}. He then calculates

$$M^{-1} \cdot \begin{pmatrix} 1 \\ 19 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \\ 4 \end{pmatrix} \pmod{26}.$$

He now knows that Alice sent the message `The...`.

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

In this “mode of operation”, one breaks a plaintext message m into blocks $m = m_1 m_2 m_3 \ldots\ldots$ Each block m_i is encrypted individually and the corresponding ciphertext is then sent.

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

In this "mode of operation", one breaks a plaintext message m into blocks $m = m_1 m_2 m_3 \ldots\ldots$ Each block m_i is encrypted individually and the corresponding ciphertext is then sent.

This is how we've introduced RSA, ElGamal, and the Hill cipher.

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

In this "mode of operation", one breaks a plaintext message m into blocks $m = m_1 m_2 m_3 \ldots\ldots$ Each block m_i is encrypted individually and the corresponding ciphertext is then sent.

This is how we've introduced RSA, ElGamal, and the Hill cipher.

Caution

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

In this "mode of operation", one breaks a plaintext message m into blocks $m = m_1 m_2 m_3 \ldots\ldots$ Each block m_i is encrypted individually and the corresponding ciphertext is then sent.

This is how we've introduced RSA, ElGamal, and the Hill cipher.

Caution

It's possible for an adversary Eve to collect known plaintext-ciphertext pairs over a long period of time.

ECB (Electronic Codebook)

The *electronic codebook* is the most direct way of implementing a block cipher.

In this "mode of operation", one breaks a plaintext message m into blocks $m = m_1 m_2 m_3 \ldots\ldots$ Each block m_i is encrypted individually and the corresponding ciphertext is then sent.

This is how we've introduced RSA, ElGamal, and the Hill cipher.

Caution

It's possible for an adversary Eve to collect known plaintext-ciphertext pairs over a long period of time.

Doing so for long enough, Eve will be able to understand messages without needing to find the decryption key of whatever cryptosystem we are using.

CBC (Cipher Block Chaining)

It's possible to implement a block cipher instead using the *cipher block chaining* mode of operation.

CBC (Cipher Block Chaining)

It's possible to implement a block cipher instead using the *cipher block chaining* mode of operation.

In this mode a plaintext message $m = m_1 m_2 m_3 \ldots$ is encrypted as follows.

CBC (Cipher Block Chaining)

It's possible to implement a block cipher instead using the *cipher block chaining* mode of operation.

In this mode a plaintext message $m = m_1 m_2 m_3 \ldots$ is encrypted as follows.

Let E_K and D_K be the encryption and decryption functions for a specific key K.

CBC (Cipher Block Chaining)

It's possible to implement a block cipher instead using the *cipher block chaining* mode of operation.

In this mode a plaintext message $m = m_1 m_2 m_3 \ldots$ is encrypted as follows.

Let E_K and D_K be the encryption and decryption functions for a specific key K.

One calculates the ciphertext $c_1 = E_K(m_1)$. Then, inductively, one calculates the jth ciphertext $c_j = E_K(m_j \oplus c_{j-1})$ where $\oplus$ is an appropriate summation operation.

CBC (Cipher Block Chaining)

It's possible to implement a block cipher instead using the *cipher block chaining* mode of operation.

In this mode a plaintext message $m = m_1 m_2 m_3 \ldots$ is encrypted as follows.

Let E_K and D_K be the encryption and decryption functions for a specific key K.

One calculates the ciphertext $c_1 = E_K(m_1)$. Then, inductively, one calculates the jth ciphertext $c_j = E_K(m_j \oplus c_{j-1})$ where $\oplus$ is an appropriate summation operation.

To decrypt, one uses the rule $m_1 = D_K(c_1)$ and $m_j = D_K(c_j) \ominus c_{j-1}$ where $\ominus$ is the opposite of $\oplus$.