Fun With Modular Encryption

Robey Holderith

Denison University - CS 271

November 15, 2005

Introduction

Modular Arithmetic Modular Encryption Xor Encryption

Properties of M. Encryption

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

Modular Encryption Tricks

Predefined Cipher Hidden Messages Scavenger Hunt

< 1[™] >

< 토 ► < 토 ►

Modular Arithmetic Modular Encryption Xor Encryption

Modular Arithmetic

Modular arithmetic is just like regular arithmetic except we wrap around a given number.

For example:

▶
$$5+6 \equiv_{10} 1$$

◆□ > ◆□ > ◆臣 > ◆臣 > ○

Modular Arithmetic Modular Encryption Xor Encryption

Modular Arithmetic

From now on assume that we are working in mod 26.

Robey Holderith Fun With Modular Encryption

< □ > < □ > < □ > < □ > < □ > .

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let $A = [a_1, a_2, \dots, a_n]$ and $B = [b_1, b_2, \dots, b_n]$. Define the following operations:

・ロン ・回と ・ヨン・

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let
$$A = [a_1, a_2, \dots, a_n]$$
 and $B = [b_1, b_2, \dots, b_n]$.
Define the following operations:

•
$$A + B = [a_1 + b_1, a_2 + b_2, \dots, a_n + b_n]$$

< □ > < □ > < □ > < □ > < □ > .

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let
$$A = [a_1, a_2, \dots, a_n]$$
 and $B = [b_1, b_2, \dots, b_n]$.
Define the following operations:

•
$$A + B = [a_1 + b_1, a_2 + b_2, \dots, a_n + b_n]$$

• $xA = [xa_1, xa_2, \dots, xa_n]$

・ロン ・回 と ・ ヨ と ・ モ と

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let
$$A = [a_1, a_2, \dots, a_n]$$
 and $B = [b_1, b_2, \dots, b_n]$.
Define the following operations:

< □ > < □ > < □ > < □ > < □ > .

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let A be our data, B be our key and C be our cipher text.

・ロン ・回 と ・ ヨ と ・ ヨ と

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let A be our data, B be our key and C be our cipher text. Encrypt $A + B \equiv C$

・ロン ・回と ・ヨン・

Modular Arithmetic Modular Encryption Xor Encryption

Modular Encryption

Let A be our data, B be our key and C be our cipher text.

Encrypt $A + B \equiv C$ Decrypt $C - B \equiv A$

・ロン ・回と ・ヨン・

Modular Arithmetic Modular Encryption Xor Encryption

Xor Encryption

Modular Encryption on $\{0,1\}$ is often called Xor Encryption.

< □ > < □ > < □ > < □ > < □ > .

Modular Arithmetic Modular Encryption Xor Encryption

Xor Encryption

Modular Encryption on $\{0,1\}$ is often called Xor Encryption.

а	b	a xor b
F	F	F
Т	F	Т
F	Т	Т
Т	Т	F

・ロン ・回 と ・ ヨ ・ ・ ヨ ・ ・

Modular Arithmetic Modular Encryption Xor Encryption

Xor Encryption

Modular Encryption on $\{0,1\}$ is often called Xor Encryption.

а	b	a xor b	â	1	b	a + b
F	F	F	C)	0	0
Т	F	Т	1		0	1
F	Т	Т	C)	1	1
Т	Т	F	1	-	1	0

◆□ > ◆□ > ◆臣 > ◆臣 > ○

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

Modular Encryption is Symmetric

(as opposed to Asymmetric)

- ► The same key is used for both encryption and decryption.
- Key must be kept secure at all times.

イロト イヨト イヨト イヨト

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

Suppose we had a message (A) and a key (B).

Α	s	е	с	r	е	t	m	е	s	s	a	g	е
В													
С													

Robey Holderith Fun With Modular Encryption

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

Suppose we had a message (A) and a key (B).

	s												
В	x	с	v	b	n	m	1	k	j	h	g	f	d
С													

Robey Holderith Fun With Modular Encryption

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

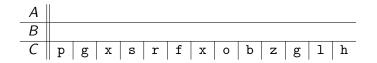
Suppose we had a message (A) and a key (B).

	s												
	x												
С	p	g	х	ຮ	r	f	x	0	b	z	g	1	h

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

Now suppose we are given C. Can we find A?



Robey Holderith Fun With Modular Encryption

・ロト ・回ト ・ヨト ・ヨト

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

Now suppose we are given C. Can we find A?

Α	0	r	a	n	g	е	0	с	t	0	b	е	r
В													
С	p	g	x	ຮ	r	f	x	0	b	z	g	1	h

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague

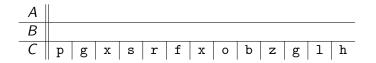
Now suppose we are given C. Can we find A?

	0												
	b												
С	p	g	х	S	r	f	x	0	b	z	g	1	h

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. II

Now suppose we are given C. Can we find A?

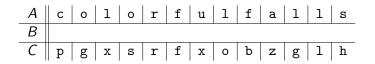


イロン イヨン イヨン イヨン

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. II

Now suppose we are given C. Can we find A?



Robey Holderith Fun With Modular Encryption

イロン 不同と 不同と 不同と

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. II

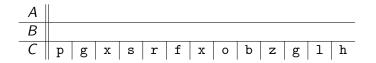
Now suppose we are given C. Can we find A?

,	A	с	0	1	ο	r	f	u	1	f	a	1	1	s
		n												-
(C	p	g	х	s	r	f	x	0	b	z	g	1	h

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. III

Now suppose we are given C. Can we find A?



Robey Holderith Fun With Modular Encryption

イロン イヨン イヨン イヨン

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. III

Now suppose we are given C. Can we find A?

Α	s	0	m	е	t	h	i	n	g	е	1	s	е
В													
С	p	g	x	s	r	f	x	0	b	z	g	1	h

Robey Holderith Fun With Modular Encryption

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

A Little Bit Vague pt. III

Now suppose we are given C. Can we find A?

		s												
		x												
-	С	p	g	х	S	r	f	x	0	b	z	g	1	h

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

So How Difficult is it to Break?

Robey Holderith Fun With Modular Encryption

< □ > < □ > < □ > < Ξ > < Ξ > ...

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

So How Difficult is it to Break?

Impossible

Robey Holderith Fun With Modular Encryption

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

So How Difficult is it to Break?

Can a single equation with two unknowns be solved?

$$A + B \equiv C$$

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

$$\blacktriangleright A + B \equiv C$$

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

- $\blacktriangleright A + B \equiv C$
- B is non-random.

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

- $\blacktriangleright A + B \equiv C$
- B is non-random.
- ▶ Given *C*, if I can find an *A* and *B* that are both non-random...

・ロト ・回ト ・ヨト ・ヨト

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

- $\blacktriangleright A + B \equiv C$
- B is non-random.
- ▶ Given *C*, if I can find an *A* and *B* that are both non-random...
- ▶ I've found the original A and B.

・ロト ・回ト ・ヨト ・ヨト

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

 $\blacktriangleright A + B \equiv C$

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

$$\blacktriangleright A + B \equiv C$$

► $D + B \equiv E$

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

$$\blacktriangleright A + B \equiv C$$

$$\blacktriangleright D + B \equiv E$$

Given C and E, I now have two equations and three unknowns.

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

$$\blacktriangleright A + B \equiv C$$

$$\blacktriangleright D + B \equiv E$$

- Given C and E, I now have two equations and three unknowns.
- But A and D must be sensical data.

・ロン ・回と ・ヨン・

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

$$\blacktriangleright A + B \equiv C$$

$$\blacktriangleright D + B \equiv E$$

- Given C and E, I now have two equations and three unknowns.
- But A and D must be sensical data.
- ▶ Look for a *B* that provides sensical *A* and *D*.

・ロト ・回ト ・ヨト ・ヨト

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

So Why Doesn't Everyone use Modular Encryption?

- When certain guidelines are met ME is unbreakable.
- Very easy to encrypt/decrypt.

・ロン ・回 と ・ ヨ と ・ ヨ と

Symmetric How Difficult is it to Break? Disposable Encryption Comparison

So Why Doesn't Everyone use Modular Encryption?

- When certain guidelines are met ME is unbreakable.
- Very easy to encrypt/decrypt.
- Keys cannot be distributed freely.
- Keys should be used multiple times sparingly.
- Keys will have a size relative to data.
- ► Asymmetric methods such as RSA are essentially unbreakable.

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher

What if I wanted to hide my message somewhere in the open? Can I make sure that my encrypted data looks like something else?

イロト イヨト イヨト イヨト

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher

What if I wanted to hide my message somewhere in the open? Can I make sure that my encrypted data looks like something else?

$$\blacktriangleright A + B \equiv C$$

・ロト ・回ト ・ヨト ・ヨト

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher

What if I wanted to hide my message somewhere in the open? Can I make sure that my encrypted data looks like something else?

$$\blacktriangleright A + B \equiv C$$

►
$$B \equiv C - A$$

イロト イヨト イヨト イヨト

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher pt. II

- Is this still secure?
- Can key be predetermined?

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher pt. II

- Is this still secure? Yes
- Can key be predetermined?

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Predefined Cipher pt. II

- Is this still secure? Yes
- Can key be predetermined? No

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Hidden Messages

Can I hide a message in my encrypted data?

・ロ・ ・ 日・ ・ 日・ ・ 日・

Predefined Cipher Hidden Messages Scavenger Hunt

Hidden Messages

Can I hide a message in my encrypted data?

▶ Let *E* be my message and *D* be the key that decodes it.

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Hidden Messages

Can I hide a message in my encrypted data?

- ▶ Let *E* be my message and *D* be the key that decodes it.
- $\blacktriangleright A + B \equiv C$

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Hidden Messages

Can I hide a message in my encrypted data?

- ▶ Let *E* be my message and *D* be the key that decodes it.
- $\blacktriangleright A + B \equiv C$
- $C D \equiv E$

イロト イヨト イヨト イヨト

Predefined Cipher Hidden Messages Scavenger Hunt

Hidden Messages

Can I hide a message in my encrypted data?

- ▶ Let *E* be my message and *D* be the key that decodes it.
- $\blacktriangleright A + B \equiv C$
- $C D \equiv E$
- $\blacktriangleright A + B D \equiv E$

イロト イヨト イヨト イヨト

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

1. Find a bunch of keys on the internet.

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

- 1. Find a bunch of keys on the internet.
- 2. Chain them together with clues.

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

- 1. Find a bunch of keys on the internet.
- 2. Chain them together with clues.
- 3. Nest each clue inside of the data so that only one clue is decrypted with each key.

イロン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

- 1. Find a bunch of keys on the internet.
- 2. Chain them together with clues.
- 3. Nest each clue inside of the data so that only one clue is decrypted with each key.
- 4. Convince the smart people at MIT that this is a good use of their time.

イロン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Scavenger Hunt/Goose Chase/Senseless Use of Time

Notice that the chain used in the previous slide can be extended.

- 1. Find a bunch of keys on the internet.
- 2. Chain them together with clues.
- 3. Nest each clue inside of the data so that only one clue is decrypted with each key.
- 4. Convince the smart people at MIT that this is a good use of their time.
- 5. Wait for someone to either win or for people to realize that this isn't really that cool.

イロン イヨン イヨン イヨン

Predefined Cipher Hidden Messages Scavenger Hunt

Thank You

Robey Holderith Fun With Modular Encryption

・ロン ・回 と ・ ヨ と ・ モ と