Fun With Modular Encryption

Robey Holderith

Denison University - CS 271

November 15, 2005

Modular Arithmetic

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

- $5 + 6 \equiv_{10} 1$
- $3 \times 8 \equiv_{10} 4$

Modular Arithmetic

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

Modular Encryption

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

Modular Encryption

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

- $A + B = [a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n]$

Modular Encryption

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

- $A + B = [a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n]$
- $xA = [xa_1, xa_2, \ldots, xa_n]$

Modular Encryption

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

- $A + B = [a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n]$
- $xA = [xa_1, xa_2, \ldots, xa_n]$
- $A - B = A + (-1)B$

Modular Encryption

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

Modular Encryption

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

Encrypt $A + B \equiv C$

Modular Encryption

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

Encrypt $A + B \equiv C$

Decrypt $C - B \equiv A$

Xor Encryption

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

Xor Encryption

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

a	b	a xor b
F	F	F
T	F	T
F	T	T
T	T	F

Xor Encryption

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

a	b	a xor b
F	F	F
T	F	T
F	T	T
T	T	F

a	b	$a + b$
0	0	0
1	0	1
0	1	1
1	1	0

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.

A Little Bit Vague

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

A	s	e	c	r	e	t	m	e	s	s	a	g	e
B													
C													

A Little Bit Vague

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

A	s	e	c	r	e	t	m	e	s	s	a	g	e
B	x	c	v	b	n	m	l	k	j	h	g	f	d
C													

A Little Bit Vague

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

A	s	e	c	r	e	t	m	e	s	s	a	g	e
B	x	c	v	b	n	m	l	k	j	h	g	f	d
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague

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

A													
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague

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

A	o	r	a	n	g	e	o	c	t	o	b	e	r
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague

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

A	o	r	a	n	g	e	o	c	t	o	b	e	r
B	b	p	x	f	l	b	j	m	i	l	f	h	q
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. II

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

A													
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. II

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

A	c	o	l	o	r	f	u	l	f	a	l	l	s
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. II

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

A	c	o	l	o	r	f	u	l	f	a	l	l	s
B	n	s	m	e	a	a	d	d	w	z	v	a	p
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. III

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

A													
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. III

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

A	s	o	m	e	t	h	i	n	g	e	l	s	e
B													
C	p	g	x	s	r	f	x	o	b	z	g	l	h

A Little Bit Vague pt. III

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

A	s	o	m	e	t	h	i	n	g	e	l	s	e
B	x	s	l	o	y	y	p	b	v	v	v	t	d
C	p	g	x	s	r	f	x	o	b	z	g	l	h

So How Difficult is it to Break?

So How Difficult is it to Break?

IMPOSSIBLE

So How Difficult is it to Break?

Can a single equation with two unknowns be solved?

$$A + B \equiv C$$

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

- $A + B \equiv C$

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

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

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

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

The Danger of Using a Non-Random Key

What happens if a non-random key is used?

- $A + B \equiv C$
- 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.

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

- $A + B \equiv C$

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

- $A + B \equiv C$
- $D + B \equiv E$

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

- $A + B \equiv C$
- $D + B \equiv E$
- Given C and E, I now have two equations and three unknowns.

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

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

The Danger of Using the Same Key Twice

What happens if the same key is used twice?

- $A + B \equiv C$
- $D + B \equiv E$
- 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.

So Why Doesn't Everyone use Modular Encryption?

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

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

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

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?

- $A + B \equiv C$

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?

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

Predefined Cipher pt. II

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

Predefined Cipher pt. II

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

Predefined Cipher pt. II

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

Hidden Messages

Can I hide a message in my encrypted data?

Hidden Messages

Can I hide a message in my encrypted data?

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

Hidden Messages

Can I hide a message in my encrypted data?

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

Hidden Messages

Can I hide a message in my encrypted data?

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

Hidden Messages

Can I hide a message in my encrypted data?

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

Scavenger Hunt/Goose Chase/Senseless Use of Time

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

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.

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.

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.

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.

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.

Thank You