Math 134: Cryptography

Lecture 2: more on ciphers

Eoin Mackall

January 8, 2024

University of California, Santa Cruz

Announcements

- Homework #1 posted on Canvas
- Syllabus updated (corrected final exam date of March 18th)
- Office hours updated (now 11:00 am - 12:00 am Tuesdays)

Last time: Shift ciphers

Alice wants to send a message to Bob.

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $j + k \pmod{26}$.

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $j + k \pmod{26}$.
3. This cipher is weak to a brute force attack because:

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:
    2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
    2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $j + k \pmod{26}$.
3. This cipher is weak to a brute force attack because:
    3.1 the keyspace is small, and it's easy to test all decryption keys,

Last time: Shift ciphers

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a secret key k, which is an integer with $1 \leq k \leq 25$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $j + k \pmod{26}$.
3. This cipher is weak to a brute force attack because:
   3.1 the keyspace is small, and it's easy to test all decryption keys,
   3.2 the likelihood of finding multiple meaningful messages testing any given decryption key is small.

Today’s plan:

1. Affine ciphers
   - Modular arithmetic
   - Affine transformations
   - Affine ciphers

Affine ciphers

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Examples

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Examples

- $6 \equiv 2 \pmod{4}$ because $6 - 2 = 4 \cdot (1)$

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Examples

- $6 \equiv 2 \pmod{4}$ because $6 - 2 = 4 \cdot (1)$
- $121 \equiv 51 \pmod{7}$ because $121 - 51 = 70 = 7 \cdot (10)$

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Examples

- $6 \equiv 2 \pmod{4}$ because $6 - 2 = 4 \cdot (1)$
- $121 \equiv 51 \pmod{7}$ because $121 - 51 = 70 = 7 \cdot (10)$
- $-13 \equiv 13 \pmod{26}$ because $-13 - 13 = -26 = 26 \cdot (-1)$

Modular arithmetic (abridged)

Let n be an integer. We're going to frequently work "modulo n".

We say two integers a, b are equivalent modulo n, or we write

$$a \equiv b \pmod{n}$$

if $a - b$ is an integer multiple of n.

Examples

- $6 \equiv 2 \pmod{4}$ because $6 - 2 = 4 \cdot (1)$
- $121 \equiv 51 \pmod{7}$ because $121 - 51 = 70 = 7 \cdot (10)$
- $-13 \equiv 13 \pmod{26}$ because $-13 - 13 = -26 = 26 \cdot (-1)$
- $81 \equiv 0 \pmod{3}$ because $81 - 0 = 81 = 3 \cdot (27)$

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,

$$a + c \equiv b + d \pmod{n}$$

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,
$$a + c \equiv b + d \pmod{n}$$
2. We can substract modulo n,

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,

$$a + c \equiv b + d \pmod{n}$$

2. We can substract modulo n,

$$a - c \equiv b - d \pmod{n}$$

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,

$$a + c \equiv b + d \pmod{n}$$

2. We can substract modulo n,

$$a - c \equiv b - d \pmod{n}$$

3. We can multiply modulo n,

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,
$$a + c \equiv b + d \pmod{n}$$
2. We can substract modulo n,
$$a - c \equiv b - d \pmod{n}$$
3. We can multiply modulo n,
$$a \cdot c \equiv b \cdot d \pmod{n}$$

Modular arithmetic (abridged)

We'll see later that the relation $*_1 \equiv *_2 \pmod{n}$ can be treated like an equality for most arithmetic purposes.

Specifically, let a, b, c, d be integers such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

1. We can add modulo n,
$$a + c \equiv b + d \pmod{n}$$
2. We can substract modulo n,
$$a - c \equiv b - d \pmod{n}$$
3. We can multiply modulo n,
$$a \cdot c \equiv b \cdot d \pmod{n}$$
4. Division is tricky.

Modular arithmetic (abridged)

Not every relation $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ (similar to matrix multiplication).

Modular arithmetic (abridged)

Not every relation $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ (similar to matrix multiplication).

Example

$4 \cdot 6 \equiv 2 \cdot 6 \pmod{6}$ since $24 - 12 = 12 = 6 \cdot (2)$.

Modular arithmetic (abridged)

Not every relation $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ (similar to matrix multiplication).

Example

$4 \cdot 6 \equiv 2 \cdot 6 \pmod{6}$ since $24 - 12 = 12 = 6 \cdot (2)$.

But $4 \not\equiv 2 \pmod{6}$ since $4 - 2 = 2 \neq 6 \cdot m$ for any integer m.

Modular arithmetic (abridged)

Not every relation $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ (similar to matrix multiplication).

Example

$4 \cdot 6 \equiv 2 \cdot 6 \pmod{6}$ since $24 - 12 = 12 = 6 \cdot (2)$.

But $4 \not\equiv 2 \pmod{6}$ since $4 - 2 = 2 \neq 6 \cdot m$ for any integer m.

Instead, for a given integer b, we can ask: when does there exist an integer that multiplies like we expect $(1/b)$ would?

Modular arithmetic (abridged)

Not every relation $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ (similar to matrix multiplication).

Example

$4 \cdot 6 \equiv 2 \cdot 6 \pmod{6}$ since $24 - 12 = 12 = 6 \cdot (2)$.

But $4 \not\equiv 2 \pmod{6}$ since $4 - 2 = 2 \neq 6 \cdot m$ for any integer m.

Instead, for a given integer b, we can ask: when does there exist an integer that multiplies like we expect $(1/b)$ would?

I.e. if we choose an integer b, then under what conditions is there an integer c such that $b \cdot c \equiv 1 \pmod{n}$?

Modular arithmetic (abridged)

Claim (to be checked later)

If b and n share no prime divisors, then there exists an integer c such that $b \cdot c \equiv 1 \pmod{n}$.

Modular arithmetic (abridged)

Claim (to be checked later)

If b and n share no prime divisors, then there exists an integer c such that $b \cdot c \equiv 1 \pmod{n}$.

Example

$15 = 3 \cdot 5$ and $26 = 2 \cdot 13$ so 15 and 26 share have no common prime divisors, so we should be able to find a multiplicative inverse for 15 modulo 26.

Modular arithmetic (abridged)

Claim (to be checked later)

If b and n share no prime divisors, then there exists an integer c such that $b \cdot c \equiv 1 \pmod{n}$.

Example

$15 = 3 \cdot 5$ and $26 = 2 \cdot 13$ so 15 and 26 share have no common prime divisors, so we should be able to find a multiplicative inverse for 15 modulo 26.

In fact,

$$15 \cdot 33 \equiv 300 + 150 + 30 + 15 \equiv 495 \equiv 19 \cdot (26) + 1 \equiv 1 \pmod{26}$$

since $(19 \cdot (26) + 1) - 1 = 19 \cdot (26)$.

Modular arithmetic (abridged)

Claim (to be checked later)

If b and n share no prime divisors, then there exists an integer c such that $b \cdot c \equiv 1 \pmod{n}$.

Example

$15 = 3 \cdot 5$ and $26 = 2 \cdot 13$ so 15 and 26 share have no common prime divisors, so we should be able to find a multiplicative inverse for 15 modulo 26.

In fact,

$$15 \cdot 33 \equiv 300 + 150 + 30 + 15 \equiv 495 \equiv 19 \cdot (26) + 1 \equiv 1 \pmod{26}$$

since $(19 \cdot (26) + 1) - 1 = 19 \cdot (26)$.

4. If b shares no common divisors with n, then we can effectively divide by b. I.e. we can find an integer c with $b \cdot c \equiv 1 \pmod{n}$ and if $x \equiv y \pmod{n}$ then $x \cdot c \equiv y \cdot c \pmod{n}$.

Affine ciphers (set-up)

Alice wants to send a message to Bob.

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:
   - 2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   - 2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $\alpha \cdot j + \beta \pmod{26}$.

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $\alpha \cdot j + \beta \pmod{26}$.

Remark

- Functions $x \mapsto \alpha x$ are often said to be linear (think of linear transformations from linear algebra).

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $\alpha \cdot j + \beta \pmod{26}$.

Remark

- Functions $x \mapsto \alpha x$ are often said to be linear (think of linear transformations from linear algebra).
- Functions $x \mapsto \alpha x + \beta$ are often called *affine* or *affine transformations*.

Affine ciphers (set-up)

Alice wants to send a message to Bob.

1. Alice and Bob agree beforehand on a pair of integers (α, β) with $1 \leq \alpha \leq 25$, $0 \leq \beta \leq 25$, and such that α is odd and $\alpha \neq 13$.
2. Plaintext is converted to ciphertext by the following scheme:
   2.1 the alphabet is enumerated (e.g. $a = 0$, $b = 1$, ..., $z = 25$)
   2.2 a plaintext letter corresponding to the value j is encrypted to the letter corresponding to value $\alpha \cdot j + \beta \pmod{26}$.

Remark

- Functions $x \mapsto \alpha x$ are often said to be linear (think of linear transformations from linear algebra).
- Functions $x \mapsto \alpha x + \beta$ are often called *affine* or *affine transformations*.
- if $\alpha = 1$ above then we just get back the shift cipher with shift β.

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$								$\cdots$			
Ciphertext								$\cdots$			

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$	7							$\cdots$			
Ciphertext								$\cdots$			

Computations

$0 \cdot 15 + 7 \equiv 7 \pmod{26}$

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$	7	22						$\cdots$			
Ciphertext								$\cdots$			

Computations

$0 \cdot 15 + 7 \equiv 7 \pmod{26}$

$1 \cdot 15 + 7 \equiv 22 \pmod{26}$

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$	7	22	11					$\cdots$			
Ciphertext								$\cdots$			

Computations

$0 \cdot 15 + 7 \equiv 7 \pmod{26}$

$1 \cdot 15 + 7 \equiv 22 \pmod{26}$

$2 \cdot 15 + 7 \equiv 37 \equiv 11 \pmod{26}$

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$	7	22	11	0	15	4	19	$\cdots$	14	3	18
Ciphertext	h	w	l	a	p	e	t	$\cdots$	o	d	s

Affine ciphers (encryption)

Example

Let's encrypt the message `This is an example of an affine cipher` using an affine cipher with scaling factor $\alpha = 15$ and shift $\beta = 7$.

Plaintext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\alpha j + \beta \pmod{26}$	7	22	11	0	15	4	19	$\cdots$	14	3	18
Ciphertext	h	w	l	a	p	e	t	$\cdots$	o	d	s

Example (cont'd)

The plaintext message `This is an example of an affine cipher` is encrypted to the ciphertext message `Gixr xr hu pohfyqp je hu heexup lxyipc`.

Affine ciphers (decryption)

Bob receives a ciphertext message from Alice. How does Bob decrypt to obtain the original plaintext message that Alice sent?

Affine ciphers (decryption)

Bob receives a ciphertext message from Alice. How does Bob decrypt to obtain the original plaintext message that Alice sent?

If Alice used the function $x \mapsto \alpha x + \beta \pmod{26}$ for her encryption, then Bob needs to find the inverse of this function, i.e. a function which takes in $y \equiv \alpha x + \beta \pmod{26}$ and outputs x.

Affine ciphers (decryption)

Bob receives a ciphertext message from Alice. How does Bob decrypt to obtain the original plaintext message that Alice sent?

If Alice used the function $x \mapsto \alpha x + \beta \pmod{26}$ for her encryption, then Bob needs to find the inverse of this function, i.e. a function which takes in $y \equiv \alpha x + \beta \pmod{26}$ and outputs x.

Let γ be an integer with $\alpha\gamma \equiv 1 \pmod{26}$, which exists since α is assumed odd and $\alpha \neq 13$.

Affine ciphers (decryption)

Bob receives a ciphertext message from Alice. How does Bob decrypt to obtain the original plaintext message that Alice sent?

If Alice used the function $x \mapsto \alpha x + \beta \pmod{26}$ for her encryption, then Bob needs to find the inverse of this function, i.e. a function which takes in $y \equiv \alpha x + \beta \pmod{26}$ and outputs x.

Let γ be an integer with $\alpha\gamma \equiv 1 \pmod{26}$, which exists since α is assumed odd and $\alpha \neq 13$.

$$\begin{aligned}
y &\equiv \alpha x + \beta \pmod{26} \\
y - \beta &\equiv \alpha x \pmod{26} \\
\gamma(y - \beta) &\equiv (\gamma\alpha)x \pmod{26} \\
\gamma(y - \beta) &\equiv 1 \cdot x \pmod{26} \\
\gamma(y - \beta) &\equiv x \pmod{26}
\end{aligned}$$

Affine ciphers (decryption)

Bob receives a ciphertext message from Alice. How does Bob decrypt to obtain the original plaintext message that Alice sent?

If Alice used the function $x \mapsto \alpha x + \beta \pmod{26}$ for her encryption, then Bob needs to find the inverse of this function, i.e. a function which takes in $y \equiv \alpha x + \beta \pmod{26}$ and outputs x.

Let γ be an integer with $\alpha\gamma \equiv 1 \pmod{26}$, which exists since α is assumed odd and $\alpha \neq 13$.

$$\begin{aligned} y &\equiv \alpha x + \beta \pmod{26} \\ \gamma(y - \beta) &\equiv x \pmod{26} \end{aligned}$$

So to decrypt, Bob calculates $\gamma(j - \beta) \pmod{26}$ for all $0 \leq j \leq 25$ and the letter corresponding to the result will yield the corresponding plaintext character.

Affine ciphers (decryption)

Example

Suppose we are told the message `Hmffg zya gyml` was gotten from an affine cipher with $(\alpha, \beta) = (3, 12)$.

Affine ciphers (decryption)

Example

Suppose we are told the message `Hmffg zya gyml` was gotten from an affine cipher with $(\alpha, \beta) = (3, 12)$.

To decrypt, we first need to find a number γ with $3 \cdot \gamma \equiv 1 \pmod{26}$. Trial and error leads to $\gamma = 9$.

Affine ciphers (decryption)

Example

Suppose we are told the message `Hmffg zya gyml` was gotten from an affine cipher with $(\alpha, \beta) = (3, 12)$.

To decrypt, we first need to find a number γ with $3 \cdot \gamma \equiv 1 \pmod{26}$. Trial and error leads to $\gamma = 9$.

Ciphertext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\gamma(j - \beta) \pmod{26}$	22	5	14	23	6	15	24	$\cdots$	21	4	13
Plaintext	w	f	o	x	g	p	y	$\cdots$	v	e	n

Affine ciphers (decryption)

Example

Suppose we are told the message `Hmffg zya gyml` was gotten from an affine cipher with $(\alpha, \beta) = (3, 12)$.

To decrypt, we first need to find a number γ with $3 \cdot \gamma \equiv 1 \pmod{26}$. Trial and error leads to $\gamma = 9$.

Ciphertext	a	b	c	d	e	f	g	$\cdots$	x	y	z
j	0	1	2	3	4	5	6	$\cdots$	23	24	25
$\gamma(j - \beta) \pmod{26}$	22	5	14	23	6	15	24	$\cdots$	21	4	13
Plaintext	w	f	o	x	g	p	y	$\cdots$	v	e	n

Example (cont'd)

The plaintext message was: `Happy new year`.

Affine ciphers (decryption)

Question

Do we really need that α is odd and $\alpha \neq 13$?

Affine ciphers (decryption)

Question

Do we really need that α is odd and $\alpha \neq 13$?

Example

Let $\alpha = 2$ and $\beta = 5$.

Affine ciphers (decryption)

Question

Do we really need that α is odd and $\alpha \neq 13$?

Example

Let $\alpha = 2$ and $\beta = 5$.

Then n, which corresponds to 13, is sent to

$$\alpha \cdot n + \beta = 2 \cdot 13 + 5 \equiv 5 \pmod{26}$$

and a, which corresponds to 0, is sent to

$$\alpha \cdot a + \beta = 2 \cdot 0 + 5 \equiv 5 \pmod{26}.$$

Affine ciphers (decryption)

Question

Do we really need that α is odd and $\alpha \neq 13$?

Example

Let $\alpha = 2$ and $\beta = 5$.

Then *n*, which corresponds to 13, is sent to

$$\alpha \cdot n + \beta = 2 \cdot 13 + 5 \equiv 5 \pmod{26}$$

and *a*, which corresponds to 0, is sent to

$$\alpha \cdot a + \beta = 2 \cdot 0 + 5 \equiv 5 \pmod{26}.$$

Without the assumption on α, our encryption isn't reversible.

Affine ciphers (security)

Benefits of Affine ciphers vs shift ciphers

Affine ciphers (security)

Benefits of Affine ciphers vs shift ciphers

- The keyspace of an affine cipher is the set of pairs (α, β). There are 12 possibilities for α and 26 possibilities for β. In total, there are 312 possible keys for an affine cipher.

Affine ciphers (security)

Benefits of Affine ciphers vs shift ciphers

- The keyspace of an affine cipher is the set of pairs (α, β). There are 12 possibilities for α and 26 possibilities for β. In total, there are 312 possible keys for an affine cipher.
- Computational cost to decrypt is now more expensive, making a brute force attack more costly.

Affine ciphers (security)

Benefits of Affine ciphers vs shift ciphers

- The keyspace of an affine cipher is the set of pairs (α, β). There are 12 possibilities for α and 26 possibilities for β. In total, there are 312 possible keys for an affine cipher.
- Computational cost to decrypt is now more expensive, making a brute force attack more costly.

This is still a pretty weak cipher though.

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Known plaintext

Suppose that Eve knows (or is told) that some specific letters of plaintext $p_1, \ldots, p_r$ correspond to some specific letters of ciphertext $c_1, \ldots, c_r$. To crack the encryption, Eve needs to solve the system

$$\begin{aligned} \alpha \cdot p_1 + \beta &\equiv c_1 \pmod{26} \\ &\vdots \\ \alpha \cdot p_r + \beta &\equiv c_r \pmod{26} \end{aligned}$$

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Known plaintext

Suppose that Eve knows (or is told) that some specific letters of plaintext $p_1, \ldots, p_r$ correspond to some specific letters of ciphertext $c_1, \ldots, c_r$. To crack the encryption, Eve needs to solve the system

$$\alpha \cdot p_1 + \beta \equiv c_1 \pmod{26}$$
$$\vdots$$
$$\alpha \cdot p_r + \beta \equiv c_r \pmod{26}$$

Most of the time, Eve will only need $r = 2$ pairs in order to solve (e.g. we only need to divide by $p_i - p_j$ for some $1 \leq i, j \leq r$ pair).

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Chosen plaintext

Suppose that Eve is allowed to choose plaintext characters and find out the corresponding ciphertext characters. Then Eve will want to find out how to encrypt a, b. This corresponds to the equations

$$\alpha \cdot 0 + \beta \equiv \beta \pmod{26} \quad \text{and} \quad \alpha \cdot 1 + \beta \equiv \alpha + \beta \pmod{26}.$$

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Chosen ciphertext

If Eve is allowed to decrypt chosen ciphertext, then Eve can choose to decrypt a, b as well. Say she gets x, y back. Then

$$\gamma(0-\beta) \equiv x \pmod{26} \quad \text{and} \quad \gamma(1-\beta) \equiv y \pmod{26}.$$

Affine ciphers (security)

Suppose Eve wants to break this cipher. Possible attacks include:

Chosen ciphertext

If Eve is allowed to decrypt chosen ciphertext, then Eve can choose to decrypt a, b as well. Say she gets x, y back. Then

$$\gamma(0-\beta) \equiv x \pmod{26} \quad \text{and} \quad \gamma(1-\beta) \equiv y \pmod{26}.$$

We can solve, $\gamma \equiv y - x \pmod{26}$, which can be used to find α. Then $-\beta \equiv \alpha x \pmod{26}$.