Classical Cryptosystems

Note

We will use the convention that plaintext will be lowercase and ciphertext will be in all capitals.

Shift Ciphers

The idea of the Caesar cipher:

- To encrypt, shift the letters to the right by 3 and wrap around.

$$
\begin{aligned}
a &\mapsto D \\
b &\mapsto E \\
x &\mapsto A
\end{aligned}
$$

Shift Ciphers

The idea of the Caesar cipher:

- To encrypt, shift the letters to the right by 3 and wrap around.

$$\begin{aligned} a &\mapsto D \\ b &\mapsto E \\ x &\mapsto A \end{aligned}$$

- To decrypt, shift the letters to the left by 3 and wrap around.

Shift Ciphers

The idea of the Caesar cipher:

- To encrypt, shift the letters to the right by 3 and wrap around.

$$
\begin{aligned}
a &\mapsto D \\
b &\mapsto E \\
x &\mapsto A
\end{aligned}
$$

- To decrypt, shift the letters to the left by 3 and wrap around.

Useful to hide message from 'friendly' agents.

A Better Version

We could choose any integer between 1 and 25 to shift, with the number being secret.

A Better Version

We could choose any integer between 1 and 25 to shift, with the number being secret.

Example

Suppose you were given

Z UVKVJK KYV PREBVVJ

with no key. How would you decrypt?

A Better Version

We could choose any integer between 1 and 25 to shift, with the number being secret.

Example

Suppose you were given

Z UVKVJK KYV PREBVVJ

with no key. How would you decrypt?

A less naive attack:

- The first letter is single, so A or I would be good to start with.

A Better Version

We could choose any integer between 1 and 25 to shift, with the number being secret.

Example

Suppose you were given

Z UVKVJK KYV PREBVVJ

with no key. How would you decrypt?

A less naive attack:

- The first letter is single, so A or I would be good to start with.
- Start with just 2-3 letters to see if it is the start of a word

Attacks

No matter the technique, this is easy to break using a ciphertext attack.

Attacks

No matter the technique, this is easy to break using a ciphertext attack.

Definition

A ciphertext attack is performed when all that is had is a copy of the ciphertext.

Attacks

No matter the technique, this is easy to break using a ciphertext attack.

Definition

A ciphertext attack is performed when all that is had is a copy of the ciphertext.

Even worse, if the attacker was performing a known-plaintext attack, they would have the decryption key while only needing a single letter.

Attacks

No matter the technique, this is easy to break using a ciphertext attack.

Definition

A ciphertext attack is performed when all that is had is a copy of the ciphertext.

Even worse, if the attacker was performing a known-plaintext attack, they would have the decryption key while only needing a single letter.

Definition

A known plaintext attack is when an attacker has a ciphertext and the corresponding plaintext. If the key is not changed, they can decrypt future ciphertexts.

Affine Ciphers

This is a method for encrypting with numbers.

Affine Ciphers

This is a method for encrypting with numbers.

Procedure

Take α, β with $0 \leq \alpha, \beta \leq 25$ such that $(\alpha, 26) = 1$. Then, the affine function

$$x \mapsto \alpha x + \beta \pmod{26}$$

It is a is a linear transformation followed by a translation.

Alternate Notation

$$E_{\alpha,\beta}(x) = (\alpha x + \beta) \pmod{26}$$

Encrypting Using Affine Ciphers

Example

$$E_{3,11}(hello) = GXSSB$$

Encrypting Using Affine Ciphers

Example

$$E_{3,11}(hello) = GXSSB$$

$$h = 7 \Rightarrow 3 \cdot 7 + 11 = 32 \equiv 6 (\text{mod } 26)$$

Encrypting Using Affine Ciphers

Example

$$E_{3,11}(hello) = GXSSB$$

$$h = 7 \Rightarrow 3 \cdot 7 + 11 = 32 \equiv 6 \pmod{26}$$
$$e = 4 \Rightarrow 3 \cdot 4 + 11 = 23 \equiv 23 \pmod{26}$$

Encrypting Using Affine Ciphers

Example

$$E_{3,11}(hello) = GXSSB$$

$$\begin{aligned} h = 7 \Rightarrow 3 \cdot 7 + 11 = 32 &\equiv 6 \pmod{26} \\ e = 4 \Rightarrow 3 \cdot 4 + 11 = 23 &\equiv 23 \pmod{26} \\ l = 11 \Rightarrow 3 \cdot 11 + 11 = 44 &\equiv 18 \pmod{26} \end{aligned}$$

Encrypting Using Affine Ciphers

Example

$$E_{3,11}(hello) = GXSSB$$

$$\begin{aligned}
h = 7 &\Rightarrow 3 \cdot 7 + 11 = 32 \equiv 6 \pmod{26} \\
e = 4 &\Rightarrow 3 \cdot 4 + 11 = 23 \equiv 23 \pmod{26} \\
l = 11 &\Rightarrow 3 \cdot 11 + 11 = 44 \equiv 18 \pmod{26} \\
o = 14 &\Rightarrow 3 \cdot 14 + 11 = 53 \equiv 1 \pmod{26}
\end{aligned}$$

Decryption with the Affine Cipher

What do we need?

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Problem?

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Problem?
We need to represent $\frac{1}{3}$ in terms of $\pmod{26}$. Since $(3, 26) = 1$, the multiplicative inverse of 3 exists modulo 26.

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Problem?
We need to represent $\frac{1}{3}$ in terms of (mod 26). Since $(3, 26) = 1$, the multiplicative inverse of 3 exists modulo 26.

$$9 \cdot 3 = 27 \equiv 1 \pmod{26}$$

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Problem?
We need to represent $\frac{1}{3}$ in terms of $\pmod{26}$. Since $(3, 26) = 1$, the multiplicative inverse of 3 exists modulo 26.

$$9 \cdot 3 = 27 \equiv 1 \pmod{26}$$

So, we can replace $\frac{1}{3}$ with 9 in our mapping.

$$x = 9(y - 11)$$

Decryption with the Affine Cipher

What do we need? Inverses ...

$$y = 3x + 11 \Rightarrow x = \frac{1}{3}(y - 11)$$

Problem?

We need to represent $\frac{1}{3}$ in terms of $\pmod{26}$. Since $(3, 26) = 1$, the multiplicative inverse of 3 exists modulo 26.

$$9 \cdot 3 = 27 \equiv 1 \pmod{26}$$

So, we can replace $\frac{1}{3}$ with 9 in our mapping.

$$x = 9(y - 11)$$

So, we see for $G = 6$, we have

$$9(6 - 11) = -45 \pmod{26} \equiv 7 \pmod{26}$$

Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$

$$l \mapsto Z$$

Can we find the key?

Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$
$$l \mapsto Z$$

Can we find the key?

First, we convert this to numerical values.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$l \mapsto Z \Rightarrow 11 \mapsto 25$$

Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$
$$l \mapsto Z$$

Can we find the key?

First, we convert this to numerical values.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$l \mapsto Z \Rightarrow 11 \mapsto 25$$

This gives

$$5\alpha + \beta \equiv 10 \pmod{26}$$
$$11\alpha + \beta \equiv 25 \pmod{26}$$

Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$

$$l \mapsto Z$$

Can we find the key?

First, we convert this to numerical values.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$l \mapsto Z \Rightarrow 11 \mapsto 25$$

This gives

$$5\alpha + \beta \equiv 10 (\text{mod } 26)$$
$$11\alpha + \beta \equiv 25 (\text{mod } 26)$$

Combining gives

$$6\alpha \equiv 15 (\text{mod } 26)$$

This will not work. Every choice for α will produce an even number and an even taken modulo 26 will always be even.

Another Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$

$$i \mapsto Z$$

Can we find the key?

Another Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$
$$i \mapsto Z$$

Can we find the key?

We begin as before.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$i \mapsto Z \Rightarrow 8 \mapsto 25$$

Another Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$
$$i \mapsto Z$$

Can we find the key?

We begin as before.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$i \mapsto Z \Rightarrow 8 \mapsto 25$$

This gives

$$5\alpha + \beta \equiv 10 (\bmod 26)$$
$$8\alpha + \beta \equiv 25 (\bmod 26)$$

Another Known Plaintext Attack

Example

Suppose we had the following plaintext-ciphertext pairs:

$$f \mapsto K$$
$$i \mapsto Z$$

Can we find the key?

We begin as before.

$$f \mapsto K \Rightarrow 5 \mapsto 10$$
$$i \mapsto Z \Rightarrow 8 \mapsto 25$$

This gives

$$5\alpha + \beta \equiv 10 \pmod{26}$$
$$8\alpha + \beta \equiv 25 \pmod{26}$$

Combining gives

$$3\alpha \equiv 15 \pmod{26}$$

Finishing the Decryption Algorithm

We can divide because $(3, 26) = 1$, so this becomes

$$\alpha \equiv 5 \pmod{26}$$

Finishing the Decryption Algorithm

We can divide because $(3, 26) = 1$, so this becomes

$$\alpha \equiv 5 \pmod{26}$$

And knowing $\alpha = 5$ gives that $\beta = 11$.

Finishing the Decryption Algorithm

We can divide because $(3, 26) = 1$, so this becomes

$$\alpha \equiv 5 \pmod{26}$$

And knowing $\alpha = 5$ gives that $\beta = 11$.

Therefore the cipher would be $5x + 11 \pmod{26}$.

What To Avoid

We have to be careful here with our choice as we need the mapping to be 1-1 modulo 26 and this only happens when $(\alpha, 26) = 1$.

What To Avoid

We have to be careful here with our choice as we need the mapping to be 1-1 modulo 26 and this only happens when $(\alpha, 26) = 1$.
Here's what happens if we aren't careful:

Suppose we try to decrypt, we get $\frac{1}{2}$ to find the inverse of. Using the other technique, we cannot find

$$a^* \ni 2a^* \equiv 1 (\text{mod } 26)$$

So, no multiplicative inverse exists. This would give a non-unique deciphering for the same ciphertext.

Improvement Over Shifts

How many keys are there for a shift cipher?

Improvement Over Shifts

How many keys are there for a shift cipher? 25

How many keys are there for an affine cipher?

Improvement Over Shifts

How many keys are there for a shift cipher? 25

How many keys are there for an affine cipher?

We could have

- possible values for α?

Improvement Over Shifts

How many keys are there for a shift cipher? 25

How many keys are there for an affine cipher?

We could have

- possible values for α? 12
- possible values for β?

Improvement Over Shifts

How many keys are there for a shift cipher? 25

How many keys are there for an affine cipher?

We could have

- possible values for α? 12
- possible values for β? 26

Improvement Over Shifts

How many keys are there for a shift cipher? 25

How many keys are there for an affine cipher?

We could have

- possible values for α? 12
- possible values for β? 26

So the total would be 312 different ciphers.

Another improvement: And, we would need two plaintext-ciphertext pairs to deduce α and β instead of one pair for a shift cipher.

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time
- Playfair ciphers permute two at a time

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time
- Playfair ciphers permute two at a time
- Invented in 1854 by Charles Wheatstone

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time
- Playfair ciphers permute two at a time
- Invented in 1854 by Charles Wheatstone
- Named after Lord Playfair, who promoted the usage

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time
- Playfair ciphers permute two at a time
- Invented in 1854 by Charles Wheatstone
- Named after Lord Playfair, who promoted the usage
- Used by British in Second Boer War and WWI

Playfair Ciphers

- Shift and affine ciphers are substitution ciphers - permute one letter at a time
- Playfair ciphers permute two at a time
- Invented in 1854 by Charles Wheatstone
- Named after Lord Playfair, who promoted the usage
- Used by British in Second Boer War and WWI
- Used by Australians and Germans in WWII

How It Works

We first need a keyword: we'll use <u>Boston</u>.

How It Works

We first need a keyword: we'll use Boston.
Letters non-distinct, we we delete all copies after first of any repeated letter. So, our keyword becomes Bostn.

How It Works

We first need a keyword: we'll use Boston.
Letters non-distinct, we we delete all copies after first of any repeated letter. So, our keyword becomes Bostn.
We construct a 5×5 grid with the keyword first and then the rest of the alphabet that is unused (with the convention $i = j$).

b	o	s	t	n
a	c	d	e	f
g	h	i	k	l
m	p	q	r	u
v	w	x	y	z

Encoding

Now we need a message to encode.

patriots will beat the jets

Encoding

Now we need a message to encode.

patriots will beat the jets

We break up the text into pairs of letters

pa tr io ts wi ll

Encoding

Now we need a message to encode.

patriots will beat the jets

We break up the text into pairs of letters

pa tr io ts wi ll

Problem ...

Encoding

Now we need a message to encode.

patriots will beat the jets

We break up the text into pairs of letters

pa	tr	io	ts	wi	ll

Problem ...

pa	tr	io	ts	wi	lx
lb	ea	tx	th	ej	et
sx					

Rules for Encoding

1. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row cyclically treated.

Rules for Encoding

1. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row cyclically treated.
2. Two plaintext letters that fall in the same column of the matrix are each replaced by the letter beneath them, with the first element of the column cyclically treated.

Rules for Encoding

1. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row cyclically treated.
2. Two plaintext letters that fall in the same column of the matrix are each replaced by the letter beneath them, with the first element of the column cyclically treated.
3. Otherwise each plaintext letter is replaced by the letter that lies in its row and column occupied by the other plaintext letter.

Example

pa is a pair from different rows and columns.

b	o	s	t	n
a	c	d	e	f
g	h	i	k	l
m	p	q	r	u
v	w	x	y	z

Each plaintext letter is replaced but the letter that lies in its row and column occupied by the other plaintext letter.

Example

pa is a pair from different rows and columns.

b	o	s	t	n
a	c	d	e	f
g	h	i	k	l
m	p	q	r	u
v	w	x	y	z

Each plaintext letter is replaced but the letter that lies in its row and column occupied by the other plaintext letter.

$$p \mapsto M$$
$$a \mapsto C$$

Example

tr is a pair in the same column.

b	o	s	t	n
a	c	d	e	f
g	h	i	k	l
m	p	q	r	u
v	w	x	y	z

Two plaintext letters that fall in the same column of the matrix are each replaced by the letter beneath them, with the first element of the column cyclically treated.

Example

tr is a pair in the same column.

b	o	s	t	n
a	c	d	e	f
g	h	i	k	l
m	p	q	r	u
v	w	x	y	z

Two plaintext letters that fall in the same column of the matrix are each replaced by the letter beneath them, with the first element of the column cyclically treated.

$$t \mapsto E$$

$$r \mapsto Y$$

Finish the ciphertext.

The Ciphertext

pa	tr	io	ts	wi	lx	MC	EY	HS	NT	XH	IZ
lb	ea	tx	th	ej	et	GN	FC	SY	OK	DK	KE
sx						DS					

The Ciphertext

pa	tr	io	ts	wi	lx		MC	EY	HS	NT	XH	IZ
lb	ea	tx	th	ej	et		GN	FC	SY	OK	DK	KE
sx							DS					

Now, we remove the spaces to finish the encryption.

MCEYHSNTXHIZGNFCSYOKDKKEDS

The Ciphertext

pa	tr	io	ts	wi	lx
lb	ea	tx	th	ej	et
sx					

MC	EY	HS	NT	XH	IZ
GN	FC	SY	OK	DK	KE
DS					

Now, we remove the spaces to finish the encryption.

MCEYHSNTXHIZGNFCSYOKDKKEDS

To decrypt, we essentially reverse the process, provided we know the key.

Weaknesses

- If the key is not known, once broken into pairs, common pairs are searched by looking for repetitive pairs and trial and error to see which common pairs it is.
  Does anyone know what pairs have the highest probability?

Weaknesses

- If the key is not known, once broken into pairs, common pairs are searched by looking for repetitive pairs and trial and error to see which common pairs it is.
  Does anyone know what pairs have the highest probability?
  Probability dictates that the common pairs are th, he, an, in, re, es.
- Another weakness is that there are only 5 possible letters for each ciphertext letter.

Weaknesses

- If the key is not known, once broken into pairs, common pairs are searched by looking for repetitive pairs and trial and error to see which common pairs it is.
  Does anyone know what pairs have the highest probability?
  Probability dictates that the common pairs are th, he, an, in, re, es.
- Another weakness is that there are only 5 possible letters for each ciphertext letter.
  This is an improvement as there are 26^2 digrams (2 letter pairs) v. only 26 letters in prior methods.

Block Ciphers

Block ciphers use symmetric keys to encrypt a string of consecutive characters through the use of matrices.

Block Ciphers

Block ciphers use symmetric keys to encrypt a string of consecutive characters through the use of matrices.

To work with these, we need a little linear algebra.

Block ciphers use symmetric keys to encrypt a string of consecutive characters through the use of matrices.

To work with these, we need a little linear algebra.

We define the inverse of a square matrix M, denoted M^{-1}, by the equation

$$MM^{-1} = M^{-1}M = I_n$$

The inverse does not always exist, but when it does this equation is satisfied.

Is the Matrix Invertible?

Easiest way to determine if M is invertible is by

Is the Matrix Invertible?

Easiest way to determine if M is invertible is by taking determinants.

Is the Matrix Invertible?

Easiest way to determine if M is invertible is by taking determinants.

Example

Determine if A is invertible.

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

Is the Matrix Invertible?

Easiest way to determine if M is invertible is by taking determinants.

Example

Determine if A is invertible.

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

$$\begin{vmatrix} 5 & 8 \\ 17 & 3 \end{vmatrix} = 5(3) - 8(17) = -121 \neq 0$$

Since $det(A) \neq 0$, A is invertible.

Finding the Inverse

Example

Find the inverse of A.

Finding the Inverse

Example

Find the inverse of A.

Using the algorithm for an 2×2 matrix. we get

$$-\frac{1}{121}\begin{bmatrix} 3 & \text{-}8 \\ \text{-}17 & 5 \end{bmatrix} \pmod{26}$$

Finding the Inverse

Example

Find the inverse of A.

Using the algorithm for an 2×2 matrix. we get

$$-\frac{1}{121}\begin{bmatrix} 3 & \text{-}8 \\ \text{-}17 & 5 \end{bmatrix} \pmod{26}$$

Problem?

Finding the Inverse

Example

Find the inverse of A.

Using the algorithm for an 2×2 matrix. we get

$$-\frac{1}{121}\begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \pmod{26}$$

Problem?

$$-121 \equiv 9 \pmod{26}$$

so we have

$$\frac{1}{9}\begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \pmod{26}$$

Finding the Inverse

Still a problem?

Finding the Inverse

Still a problem?

$$3 \cdot 9 \equiv 1 \pmod{26}$$

we can replace $\frac{1}{9}$ by 3 to get

$$3 \begin{bmatrix} 3 & \text{-8} \\ \text{-17} & 5 \end{bmatrix} \pmod{26}$$

Finding the Inverse

Still a problem?

$$3 \cdot 9 \equiv 1 \pmod{26}$$

we can replace $\frac{1}{9}$ by 3 to get

$$3 \begin{bmatrix} 3 & \text{-8} \\ \text{-17} & 5 \end{bmatrix} \pmod{26}$$

Done?

Finding the Inverse

Still a problem?

$$3 \cdot 9 \equiv 1 (\mathrm{mod}\ 26)$$

we can replace $\frac{1}{9}$ by 3 to get

$$3 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} (\mathrm{mod}\ 26)$$

Done?

$$\begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} (\mathrm{mod}\ 26)$$

Finding the Inverse

Still a problem?

$$3 \cdot 9 \equiv 1 \pmod{26}$$

we can replace $\frac{1}{9}$ by 3 to get

$$3 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \pmod{26}$$

Done?

$$\begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} \pmod{26}$$

Now?

Finding the Inverse

Still a problem?

$$3 \cdot 9 \equiv 1 \pmod{26}$$

we can replace $\frac{1}{9}$ by 3 to get

$$3 \begin{bmatrix} 3 & \text{-}8 \\ \text{-}17 & 5 \end{bmatrix} \pmod{26}$$

Done?

$$\begin{bmatrix} 9 & \text{-}24 \\ \text{-}51 & 15 \end{bmatrix} \pmod{26}$$

Now?

$$A^{-1} = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}$$

The Hill Algorithm

This is named after Lester Hill, who produced work in 1929.

The encryption algorithm takes m successive plaintext letters and substitutes them for m ciphertext letters. This substitution is determined by m linear equations in which each character is assigned a numerical value ($a = 0, b = 1, \ldots$).

How the Hill Cipher Works

For $m = 3$, the system of equations can be described as

$$\begin{aligned}
c_1 &= (k_{11}p_1 + k_{12}p_1 + k_{13}p_1)\pmod{26} \\
c_2 &= (k_{21}p_2 + k_{22}p_2 + k_{23}p_2)\pmod{26} \\
c_3 &= (k_{31}p_3 + k_{32}p_3 + k_{33}p_3)\pmod{26}
\end{aligned}$$

How the Hill Cipher Works

For $m = 3$, the system of equations can be described as

$$\begin{aligned} c_1 &= (k_{11}p_1 + k_{12}p_1 + k_{13}p_1) \pmod{26} \\ c_2 &= (k_{21}p_2 + k_{22}p_2 + k_{23}p_2) \pmod{26} \\ c_3 &= (k_{31}p_3 + k_{32}p_3 + k_{33}p_3) \pmod{26} \end{aligned}$$

This can now be expressed in terms of vectors and matrices

$$\begin{bmatrix} c_1 & c_2 & c_3 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 & p_3 \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \pmod{26}$$

where c and p are vectors of length 3 representing the **p**laintext and associated **c**iphertext.

Using the Hill Algorithm

Example

Using the encryption key

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

encrypt ‘pay more money’.

Using the Hill Algorithm

Example

Using the encryption key

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

encrypt 'pay more money'.

The first 3 letters of the plaintext are represented by the vector

$$\begin{bmatrix} 15 & 0 & 24 \end{bmatrix}$$

Using the Hill Algorithm

Then,

$$\begin{bmatrix} 15 & 0 & 24 \end{bmatrix} K = \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \pmod{26}$$

Using the Hill Algorithm

Then,

$$\begin{bmatrix} 15 & 0 & 24 \end{bmatrix} K = \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \pmod{26}$$

Which, when take modulo 26, becomes

$$\begin{bmatrix} 17 & 17 & 11 \end{bmatrix}$$

and this corresponds to RRL.

Using the Hill Algorithm

Then,

$$\begin{bmatrix} 15 & 0 & 24 \end{bmatrix} K = \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \pmod{26}$$

Which, when take modulo 26, becomes

$$\begin{bmatrix} 17 & 17 & 11 \end{bmatrix}$$

and this corresponds to RRL.
Continuing in this way, the ciphertext for the whole plaintext is

RRLMWBKASPDH

Decryption with the Hill Cipher

Decryption requires using the inverse of the matrix K. First,

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} = 23 \neq 0$$

Decryption with the Hill Cipher

Decryption requires using the inverse of the matrix K. First,

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} = 23 \neq 0$$

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

when taken modulo 26.

Decryption with the Hill Cipher

Decryption requires using the inverse of the matrix K. First,

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} = 23 \neq 0$$

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

when taken modulo 26.
If K^{-1} is applied to the ciphertext, then the plaintext is easily recovered.

$$\begin{bmatrix} 17 & 17 & 11 \end{bmatrix} K^{-1} = \begin{bmatrix} 587 & 442 & 544 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 15 & 0 & 24 \end{bmatrix}$$

What’s Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.

What's Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.

As with Hill, the use of larger matrices hides more frequency information.

What's Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.

As with Hill, the use of larger matrices hides more frequency information.

For example, $K \in \mathcal{M}_3$ hides 2 letter frequencies.

What's Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.

As with Hill, the use of larger matrices hides more frequency information.

For example, $K \in \mathcal{M}_3$ hides 2 letter frequencies.

Although the Hill cipher is strong against the cipher-only attack, it is easily broken down with a known plaintext attack.

What's Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.

As with Hill, the use of larger matrices hides more frequency information.

For example, $K \in \mathcal{M}_3$ hides 2 letter frequencies.

Although the Hill cipher is strong against the cipher-only attack, it is easily broken down with a known plaintext attack.

If we have an $m \times m$ Hill cipher, suppose we have m plaintext-ciphertext pairs, each of length m. We label the pairs $\overrightharpoon{P}_j = (p_{1j}, p_{2j}, \ldots, p_{mj})$ and $\overrightharpoon{C}_j = (c_{1j}, c_{2j}, \ldots, c_{mj})$ such that $\overrightharpoon{C}_j = \overrightharpoon{P}_j K$ for $1 \le j \le m$ and for some unknown key matrix K.

What's Good and Bad

As with the Playfair cipher, the strength of the Hill cipher is that it completely hides single letter frequencies.
As with Hill, the use of larger matrices hides more frequency information.
For example, $K \in \mathcal{M}_3$ hides 2 letter frequencies.
Although the Hill cipher is strong against the cipher-only attack, it is easily broken down with a known plaintext attack.
If we have an $m \times m$ Hill cipher, suppose we have m plaintext-ciphertext pairs, each of length m. We label the pairs $\overrightharpoon{P}_j = (p_{1j}, p_{2j}, \ldots, p_{mj})$ and $\overrightharpoon{C}_j = (c_{1j}, c_{2j}, \ldots, c_{mj})$ such that $\overrightharpoon{C}_j = \overrightharpoon{P}_j K$ for $1 \leq j \leq m$ and for some unknown key matrix K.
Now, define $X, Y \in \mathcal{M}_m$ such that $X = (p_{ij})$ and $Y = (c_{ij})$. Then we can form the equation $Y = XK$. If X is invertible, $K = X^{-1}Y$ and we are done. If not, then a new version of X can be formed with additional plaintext-ciphertext pairs until and invertible X is obtained.

Cracking the Hill Algorithm

Example

Suppose the plaintext 'hill cipher' is encrypted using a 2×2 Hill cipher to yield the ciphertext HCRZSSXNSP. Find the encryption key.

Example

Suppose the plaintext 'hill cipher' is encrypted using a 2×2 Hill cipher to yield the ciphertext HCRZSSXNSP. Find the encryption key.

Based on the plaintext-cipher text pairs we have, we can set up the following:

$$\begin{bmatrix} 7 & 8 \end{bmatrix} K \pmod{26} = \begin{bmatrix} 7 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 11 \end{bmatrix} K \pmod{26} = \begin{bmatrix} 17 & 25 \end{bmatrix}$$

and so forth.

Cracking the Hill Algorithm

Using the first two plaintext-ciphertext pairs, we have

$$\begin{bmatrix} 7 & 2 \\ 17 & 25 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} K \pmod{26}$$

Using the first two plaintext-ciphertext pairs, we have

$$\begin{bmatrix} 7 & 2 \\ 17 & 25 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} K (\text{mod } 26)$$

Now, we need to find the inverse of P. Since this is a 2×2 system, we have the following algorithm:

$$P^{-1} = \begin{bmatrix} \text{a} & \text{b} \\ \text{d} & \text{d} \end{bmatrix}^{-1} = \frac{1}{det(P)} \begin{bmatrix} \text{d} & \text{-b} \\ \text{-c} & \text{a} \end{bmatrix}$$

Cracking the Hill Algorithm

If P^{-1} exists, then $|P| \neq 0$. Here ,

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = -11 \neq 0$$

Cracking the Hill Algorithm

If P^{-1} exists, then $|P| \neq 0$. Here ,

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = -11 \neq 0$$

So, we have that

$$P^{-1} = \frac{1}{-11} \begin{bmatrix} 11 & \text{-8} \\ \text{-11} & 7 \end{bmatrix} \pmod{26}$$

Cracking the Hill Algorithm

We need to rewrite modulo 26, which means no negatives and no fractions.

We need to rewrite modulo 26, which means no negatives and no fractions.
First, $-11 \equiv 15 (\mathrm{mod}\ 26)$, so we can replace $\frac{1}{-11}$ with $\frac{1}{15}$. Next, we need to represent $\frac{1}{15}$ as an integer.

Cracking the Hill Algorithm

We need to rewrite modulo 26, which means no negatives and no fractions.
First, $-11 \equiv 15 \pmod{26}$, so we can replace $\frac{1}{-11}$ with $\frac{1}{15}$. Next, we need to represent $\frac{1}{15}$ as an integer.
To do so, consider that $15 \cdot \frac{1}{15} \equiv 1 \pmod{26}$. So what we need is an integer such that the product of that integer and 15 is congruent to 1 modulo 26. Here, the integer we seek is 7.

Cracking the Hill Algorithm

At this point we now have

$$P^{-1} = 7 \begin{bmatrix} 11 & \text{-8} \\ \text{-11} & 7 \end{bmatrix} \pmod{26}$$

Cracking the Hill Algorithm

At this point we now have

$$P^{-1} = 7 \begin{bmatrix} 11 & \text{-}8 \\ \text{-}11 & 7 \end{bmatrix} \pmod{26}$$

We multiply through to get

$$P^{-1} = \begin{bmatrix} 77 & \text{-}56 \\ \text{-}77 & 49 \end{bmatrix} \pmod{26}$$

Cracking the Hill Algorithm

At this point we now have

$$P^{-1} = 7\begin{bmatrix} 11 & \text{-8} \\ \text{-11} & 7 \end{bmatrix} \pmod{26}$$

We multiply through to get

$$P^{-1} = \begin{bmatrix} 77 & \text{-56} \\ \text{-77} & 49 \end{bmatrix} \pmod{26}$$

And finally, when we take this modulo 26, we get

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}^{-1} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

Cracking the Hill Algorithm

So,

$$K = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} 7 & 2 \\ 17 & 25 \end{bmatrix} = \begin{bmatrix} 549 & 600 \\ 398 & 577 \end{bmatrix} \pmod{26}$$

Cracking the Hill Algorithm

So,

$$K = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{bmatrix} 7 & 2 \\ 17 & 25 \end{bmatrix} = \begin{bmatrix} 549 & 600 \\ 398 & 577 \end{bmatrix} \pmod{26}$$

Which reduces to

$$K = \begin{bmatrix} 3 & 2 \\ 8 & 5 \end{bmatrix}$$

How many of you remember what a permutation is from abstract algebra?

Permutation Ciphers

How many of you remember what a permutation is from abstract algebra?

Definition

A permutation $\pi : S \to S$ such that π is a bijection.

Permutation Ciphers

How many of you remember what a permutation is from abstract algebra?

Definition

A permutation $\pi : S \to S$ such that π is a bijection.

We can use permutations to encrypt plaintext by arranging the letters in blocks of an appropriate length and then permuting within each one.

Permutation Cipher Example

Example

If our plaintext is ‘lets go black and gold’, use the permutation $\pi = (13)(254)$ to encrypt.

Permutation Cipher Example

Example

If our plaintext is 'lets go black and gold', use the permutation $\pi = (13)(254)$ to encrypt.

The length of the permutation tells us that we want to break the plaintext into blocks of length 5.

letsg oblac kandg oldxx

Permutation Cipher Example

Example

If our plaintext is ‘lets go black and gold’, use the permutation $\pi = (13)(254)$ to encrypt.

The length of the permutation tells us that we want to break the plaintext into blocks of length 5.

letsg oblac kandg oldxx

Next, apply π to each block.

letsg	oblac	kandg	oldxx
tgles	lcoba	ngkad	dxolx

Permutation Cipher Example

Example

If our plaintext is 'lets go black and gold', use the permutation $\pi = (13)(254)$ to encrypt.

The length of the permutation tells us that we want to break the plaintext into blocks of length 5.

letsg oblac kandg oldxx

Next, apply π to each block.

letsg	oblac	kandg	oldxx
tgles	lcoba	ngkad	dxolx

Finally, we have

TGLESLCOBANGKADDXOLX

Decryption of the Permutation Cipher

To decrypt, we need to find the inverse of the permutation and apply it to the cipher text.

Decryption of the Permutation Cipher

To decrypt, we need to find the inverse of the permutation and apply it to the cipher text.

Do we remember how to find the inverse of a permutation?

Example

Find π^{-1} for $\pi = (13)(254)$.

Decryption of the Permutation Cipher

To decrypt, we need to find the inverse of the permutation and apply it to the cipher text.
Do we remember how to find the inverse of a permutation?

Example

Find π^{-1} for $\pi = (13)(254)$.

We reverse the cycles and invert the order.

$$\pi^{-1} = (452)(31) = (452)(13)$$

Attacks on the Permutation Cipher

- This cipher is easily beatable with a known plaintext attack

Attacks on the Permutation Cipher

- This cipher is easily beatable with a known plaintext attack
- We could also use brute force

Attacks on the Permutation Cipher

- This cipher is easily beatable with a known plaintext attack
- We could also use brute force

Definition

A brute force attack involves trying all possible arrangements of the letters in a ciphertext to find the associated plaintext

Decryption with the Permutation Cipher

Example

Decrypt

TGLESLCOBANGKADDXOLX

with only the knowledge that it was encrypted with a permutation cipher.

Decryption with the Permutation Cipher

Example

Decrypt

TGLESLCOBANGKADDXOLX

with only the knowledge that it was encrypted with a permutation cipher.

Where do we start?

Decryption with the Permutation Cipher

Example

Decrypt

TGLESLCOBANGKADDXOLX

with only the knowledge that it was encrypted with a permutation cipher.

Where do we start?
Size of blocks must be divisor of 20.

Decryption with the Permutation Cipher

Example

Decrypt

TGLESLCOBANGKADDXOLX

with only the knowledge that it was encrypted with a permutation cipher.

Where do we start?
Size of blocks must be divisor of 20.
Why can we rule out key size 2?

Decryption with the Permutation Cipher

Example

Decrypt

TGLESLCOBANGKADDXOLX

with only the knowledge that it was encrypted with a permutation cipher.

Where do we start?
Size of blocks must be divisor of 20.
Why can we rule out key size 2?
No two letter words made up of T and G.

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?
No, since the first 4 letters are TGLE, which could give 'GET L'

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?
No, since the first 4 letters are TGLE, which could give ‘GET L’

T	G	L	E
S	L	C	O
B	A	N	G
K	A	D	D
X	O	L	X

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?
No, since the first 4 letters are TGLE, which could give 'GET L'

T	G	L	E
S	L	C	O
B	A	N	G
K	A	D	D
X	O	L	X

Notice the last row and the X's ...

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?
No, since the first 4 letters are TGLE, which could give 'GET L'

T	G	L	E
S	L	C	O
B	A	N	G
K	A	D	D
X	O	L	X

Notice the last row and the X's ...
Possible last rows: OLXX and LOXX

Decryption with the Permutation Cipher

Next we try key length 4. Can we instantly rule this out?
No, since the first 4 letters are TGLE, which could give 'GET L'

T	G	L	E
S	L	C	O
B	A	N	G
K	A	D	D
X	O	L	X

Notice the last row and the X's ...
Possible last rows: OLXX and LOXX
Possible 4^{th} rows: ADKD, ADDK, DAKD and DADK

Decryption with the Permutation Cipher

We look at the first 5 letters and we see that we have LETS G, so we cannot rule out 5 for a length. We again set up an array.

T	G	L	E	S
L	C	O	B	A
N	G	K	A	D
D	X	O	L	X

Decryption with the Permutation Cipher

We look at the first 5 letters and we see that we have LETS G, so we cannot rule out 5 for a length. We again set up an array.

T	G	L	E	S
L	C	O	B	A
N	G	K	A	D
D	X	O	L	X

If we begin with LETS G, we arrange the other rows using the same permutation.

l	e	t	s	g
o	b	l	a	c
k	a	n	d	g
o	l	d	x	x

And if we rewrite with appropriate spacing, we'd have our plaintext.

Column Permutation Ciphers

We again are using a permutation, and the initial encoding is not that unlike the permutation cipher. The difference is, instead of just permuting a block, we permute all of them simultaneously and then write the ciphertext by taking the columns in the same orientation as the permutation.

Example

Using the permutation $\pi = (13)(24)$, encrypt the message

this is a sample plaintext

Encrypting with a Column Permutation Cipher

First we arrange the plaintext into an array with rows of length 4.

t	h	i	s
i	s	a	s
a	m	p	l
e	p	l	a
i	n	t	e
x	t	x	x

with padding at the end to make all rows the same length.

Encrypting with a Column Permutation Cipher

Then we permute based on π.

3	4	1	2
t	h	i	s
i	s	a	s
a	m	p	l
e	p	l	a
i	n	t	e
x	t	x	x

Encrypting with a Column Permutation Cipher

Then we permute based on π.

3	4	1	2
t	h	i	s
i	s	a	s
a	m	p	l
e	p	l	a
i	n	t	e
x	t	x	x

The corresponding ciphertext is

IAPLTXSSLAEXTIAEIXHSMPNT

Decryption with a Column Permutation Cipher

Here again, we know the key length must be a divisor of the number of characters in the ciphertext. In our last example, the length is 24, so we know there are 2,3,4,6,8,12 or 24 columns.

Decryption with a Column Permutation Cipher

Here again, we know the key length must be a divisor of the number of characters in the ciphertext. In our last example, the length is 24, so we know there are 2,3,4,6,8,12 or 24 columns.

Here is a trick to guess this key length - 40% of letters in any stretch of English text are vowels. So we can use probability to help us. We can arrange into a number of columns and do a frequency analysis to see if it makes sense.

Decryption Example with a Column Permutation Cipher

Example

If we know the following Ciphertext was encrypted usIng a column Permutation cipHer, decodE the cipheRtext.

> *WEDENODTURTKRHNSUKUXNSOSOIJOQR*
> *HYGWGRHTTTEAEATHEOAEHEGIFISOAX*

Decryption Example with a Column Permutation Cipher

Example

If we know the following Ciphertext was encrypted usIng a column Permutation cipHer, decodE the cipheRtext.

> *WEDENODTURTKRHNSUKUXNSOSOIJOQR*
> *HYGWGRHTTTEAEATHEOAEHEGIFISOAX*

There are 60 characters here, so we know the number of columns is a divisor of 60.

Decryption Example with a Column Permutation Cipher

Example

If we know the following Ciphertext was encrypted usIng a column Permutation cipHer, decodE the cipheRtext.

WEDENODTURTKRHNSUKUXNSOSOIJOQR
HYGWGRHTTTEAEATHEOAEHEGIFISOAX

There are 60 characters here, so we know the number of columns is a divisor of 60.
60 is a small number, so frequency analysis may be tough since there is such a small sample size.

Be Clever with Attacks

WEDENODTURTKRHNSUKUXNSOSOIJOQR
HYGWGRHTTTEAEATHEOAEHEGIFISOAX

Be Clever with Attacks

WEDENODTURTKRHNSUKUXNSOSOIJOQR
HYGWGRHTTTEAEATHEOAEHEGIFISOAX

The 20^{th} and 60^{th} letter are both X, so we may guess that those were null letters at the bottom of columns.

Be Clever with Attacks

WEDENODTURTKRHNSUKUXNSOSOIJOQR
HYGWGRHTTTEAEATHEOAEHEGIFISOAX

The 20^{th} and 60^{th} letter are both X, so we may guess that those were null letters at the bottom of columns.
Good choices for the number of columns?

Be Clever with Attacks

WEDENODTURTKRHNSUKUXNSOSOIJOQR
HYGWGRHTTTEAEATHEOAEHEGIFISOAX

The 20^{th} and 60^{th} letter are both X, so we may guess that those were null letters at the bottom of columns.
Good choices for the number of columns?
The number of rows is a divisor of 60 and a multiple of 10. That would leave us with 10, 20 or 30 rows.

Decryption with a Column Permutation Cipher

So let's start with 10, which would mean there are 6 columns.

W	T	N	H	E	H
E	K	S	Y	A	E
D	R	O	G	E	G
E	H	S	W	A	I
N	N	O	G	T	F
O	S	I	R	H	I
D	U	J	H	E	S
T	K	O	T	O	O
U	U	Q	T	A	A
R	X	R	T	E	X

Decryption with a Column Permutation Cipher

Then, we reorder them with the two columns that end in X as the last two. From there, we want to permute the first four columns until we find an arrangement that makes sense.

Decryption with a Column Permutation Cipher

Then, we reorder them with the two columns that end in X as the last two. From there, we want to permute the first four columns until we find an arrangement that makes sense.

w	h	e	n	t	h
e	y	a	s	k	e
d	g	e	o	r	g
e	w	a	s	h	i
n	g	t	o	n	f
o	r	h	i	s	i
d	h	e	j	u	s
t	t	o	o	k	o
u	t	a	q	u	a
r	t	e	r	x	x

Decryption with a Column Permutation Cipher

Then, we reorder them with the two columns that end in X as the last two. From there, we want to permute the first four columns until we find an arrangement that makes sense.

w	h	e	n	t	h
e	y	a	s	k	e
d	g	e	o	r	g
e	w	a	s	h	i
n	g	t	o	n	f
o	r	h	i	s	i
d	h	e	j	u	s
t	t	o	o	k	o
u	t	a	q	u	a
r	t	e	r	x	x

when they asked george washington for his id, he just took out a quarter.

Double Transposition Cipher

- Here we take the original plaintext P and encipher it using a column transposition with one keyword creating an intermediate ciphertext C'

Double Transposition Cipher

- Here we take the original plaintext P and encipher it using a column transposition with one keyword creating an intermediate ciphertext C'
- Then we will encipher C' using a second keyword in a column transposition creating the final ciphertext C

Double Transposition Cipher

- Here we take the original plaintext P and encipher it using a column transposition with one keyword creating an intermediate ciphertext C'
- Then we will encipher C' using a second keyword in a column transposition creating the final ciphertext C
- It is not necessary for the two keywords to be of the same length

Double Transposition Cipher

- Here we take the original plaintext P and encipher it using a column transposition with one keyword creating an intermediate ciphertext C'
- Then we will encipher C' using a second keyword in a column transposition creating the final ciphertext C
- It is not necessary for the two keywords to be of the same length
- If necessary, we can pad C' with null characters so that it becomes the appropriate length

Double Transposition Cipher Example

Example

Suppose we wanted to encrypt the plaintext

it better stop raining before the game

using a double transposition cipher with keywords redsox and baseball. Find the ciphertext.

Double Transposition Cipher Example

Example

Suppose we wanted to encrypt the plaintext

it better stop raining before the game

using a double transposition cipher with keywords redsox and baseball. Find the ciphertext.

First, we arrange the plaintext in an array with rows of length 6.

i	t	b	e	t	t
e	r	s	t	o	p
r	a	i	n	i	n
g	b	e	f	o	r
e	t	h	e	g	a
m	e	x	x	x	x

Why did we use 6 for the row length?

Double Transposition Cipher Example

Example

Suppose we wanted to encrypt the plaintext

it better stop raining before the game

using a double transposition cipher with keywords redsox and baseball. Find the ciphertext.

First, we arrange the plaintext in an array with rows of length 6.

i	t	b	e	t	t
e	r	s	t	o	p
r	a	i	n	i	n
g	b	e	f	o	r
e	t	h	e	g	a
m	e	x	x	x	x

Why did we use 6 for the row length? That is the length of our first keyword.

Double Transposition Cipher Example

R	E	D	S	O	X
i	t	b	e	t	t
e	r	s	t	o	p
r	a	i	n	i	n
g	b	e	f	o	r
e	t	h	e	g	a
m	e	x	x	x	x

Double Transposition Cipher Example

Now we include numerical values.

R	E	D	S	O	X
4	2	1	5	3	6
i	t	b	e	t	t
e	r	s	t	o	p
r	a	i	n	i	n
g	b	e	f	o	r
e	t	h	e	g	a
m	e	x	x	x	x

Double Transposition Cipher Example

Now we include numerical values.

R	E	D	S	O	X
4	2	1	5	3	6
i	t	b	e	t	t
e	r	s	t	o	p
r	a	i	n	i	n
g	b	e	f	o	r
e	t	h	e	g	a
m	e	x	x	x	x

Now, we get our intermediate ciphertext by taking the columns in order.
C': BSIEHXTRABTETOIOGXIERGEMETNFEXTPNRAX

Double Transposition Cipher Example

Now we take this ciphertext and make a new array with this broken into rows of length 8.

Double Transposition Cipher Example

Now we take this ciphertext and make a new array with this broken into rows of length 8.

B	S	I	E	H	X	T	R
A	B	T	E	T	O	I	O
G	X	I	E	R	G	E	M
E	T	N	F	E	X	T	P
N	R	A	X	Z	Z	Z	Z

Double Transposition Cipher Example

B	A	S	E	B	A	L	L
B	S	I	E	H	X	T	R
A	B	T	E	T	O	I	O
G	X	I	E	R	G	E	M
E	T	N	F	E	X	T	P
N	R	A	X	Z	Z	Z	Z

Double Transposition Cipher Example

B	A	S	E	B	A	L	L
3	1	8	5	4	2	6	7
B	S	I	E	H	X	T	R
A	B	T	E	T	O	I	O
G	X	I	E	R	G	E	M
E	T	N	F	E	X	T	P
N	R	A	X	Z	Z	Z	Z

We now do the same with this keyword as we did with the last one. Since there is repetition of letters, we assign the smaller value to the one that appears first in the keyword.

Double Transposition Cipher Example

B	A	S	E	B	A	L	L
3	1	8	5	4	2	6	7
B	S	I	E	H	X	T	R
A	B	T	E	T	O	I	O
G	X	I	E	R	G	E	M
E	T	N	F	E	X	T	P
N	R	A	X	Z	Z	Z	Z

We now do the same with this keyword as we did with the last one. Since there is repetition of letters, we assign the smaller value to the one that appears first in the keyword.
Now we take the columns in numerical order to get our final ciphertext.
C: SBXTRXOGXZBAGENHTREZEEEFXTIETZROMPZITINA

Cryptanalysis on Double Transposition Ciphers

- collect several ciphertexts of the same length and line them up, one right underneath the other

Cryptanalysis on Double Transposition Ciphers

- collect several ciphertexts of the same length and line them up, one right underneath the other
- Then attempt to permute the columns in such a way that all of the rows make sense

Cryptanalysis on Double Transposition Ciphers

- collect several ciphertexts of the same length and line them up, one right underneath the other
- Then attempt to permute the columns in such a way that all of the rows make sense
- it still makes sense to try to utilize the information about the percentage of vowels in a piece of English

Cryptanalysis on Double Transposition Ciphers

- collect several ciphertexts of the same length and line them up, one right underneath the other
- Then attempt to permute the columns in such a way that all of the rows make sense
- it still makes sense to try to utilize the information about the percentage of vowels in a piece of English
- there are many more letters to permute, the task is most definitely much more difficult than breaking a single column transposition

Can You Decipher?

Example

Suppose you intercepted the following message:

YRGSFCGUBANILNNRDLGOCLE
XNEATRAHHLAEOOITXAGUAOETT

You think it is a quote from a famous comedian. Decipher this ciphertext.

Solution

We have to realize that this is a column permutation cipher and that the code word is ‘Carlin’. Once we do, we see that we should set this up with 6 columns.

Solution

We have to realize that this is a column permutation cipher and that the code word is 'Carlin'. Once we do, we see that we should set this up with 6 columns.

Y	B	D	N	L	A
R	A	L	E	A	G
G	N	G	A	E	U
S	I	O	T	O	A
F	L	C	R	O	O
C	N	L	A	I	E
G	N	E	H	T	T
U	R	X	H	X	T

Solution

Now, we can use the code word Carlin.

A	C	I	L	N	R
Y	B	D	N	L	A
R	A	L	E	A	G
G	N	G	A	E	U
S	I	O	T	O	A
F	L	C	R	O	O
C	N	L	A	I	E
G	N	E	H	T	T
U	R	X	H	X	T

Solution

When we reorder, we get

C	A	R	L	I	N
b	y	a	n	d	l
a	r	g	e	l	a
n	g	u	a	g	e
i	s	a	t	o	o
l	f	o	r	c	o
n	c	e	a	l	i
n	g	t	h	e	t
r	u	t	h	x	x

Solution

When we reorder, we get

C	A	R	L	I	N
b	y	a	n	d	l
a	r	g	e	l	a
n	g	u	a	g	e
i	s	a	t	o	o
l	f	o	r	c	o
n	c	e	a	l	i
n	g	t	h	e	t
r	u	t	h	x	x

Which gives us

By and large, language is a tool for concealing the truth.

Another Decryption

Example

Find the plaintext for the following ciphertext, given that a double transposition cipher was used, and it is attributed to an Unknown Athlete.

NELT NXCHU PITT IRCRA OTYA WNEUXL OGUG EXLCI TOUT ODTTI NYRG PIIIE TCGN ATRT

Solution

The keywords we need here are unknown and athlete. We first count to see that there are 63 characters, and since the keyword ‘athlete’ has 7 letters, we need 9 rows. So, we break this ciphertext into sets of 9 and make them the columns.

Solution

The keywords we need here are unknown and athlete. We first count to see that there are 63 characters, and since the keyword 'athlete' has 7 letters, we need 9 rows. So, we break this ciphertext into sets of 9 and make them the columns.

N	P	O	L	I	I	E
E	I	T	O	T	N	T
L	T	Y	G	O	Y	C
T	T	A	U	U	R	G
N	I	W	G	T	G	N
X	R	N	E	O	P	A
C	C	E	X	D	I	T
H	R	U	L	T	I	R
U	A	X	C	T	I	T

Solution

Now we use the keyword to see how to rearrange.

A	E	E	H	L	T	T
N	P	O	L	I	I	E
E	I	T	O	T	N	T
L	T	Y	G	O	Y	C
T	T	A	U	U	R	G
N	I	W	G	T	G	N
X	R	N	E	O	P	A
C	C	E	X	D	I	T
H	R	U	L	T	I	R
U	A	X	C	T	I	T

Solution

A	T	H	L	E	T	E
N	I	L	I	P	E	O
E	N	O	T	I	T	T
L	Y	G	O	T	C	Y
T	R	U	U	T	G	A
N	G	G	T	I	N	W
X	P	E	O	R	A	N
C	I	X	D	C	T	E
H	I	L	T	R	R	U
U	I	C	T	A	T	X

Solution

A	T	H	L	E	T	E
N	I	L	I	P	E	O
E	N	O	T	I	T	T
L	Y	G	O	T	C	Y
T	R	U	U	T	G	A
N	G	G	T	I	N	W
X	P	E	O	R	A	N
C	I	X	D	C	T	E
H	I	L	T	R	R	U
U	I	C	T	A	T	X

This gives the intermediate ciphertext

NILIPEOENOTITTLYGOTCYTRUUTGANGG
TINWXPEORANCIXDCTEHILTRRUUICTATX

Solution

And now we have another keyword with 7 letters, so we use this ciphertext to write the 9 rows of the next grid.

Solution

And now we have another keyword with 7 letters, so we use this ciphertext to write the 9 rows of the next grid.

N	O	T	A	P	D	R
I	T	C	N	E	C	U
L	I	Y	G	O	T	U
I	T	T	G	R	E	I
P	T	R	T	A	H	C
E	L	U	I	N	I	T
O	Y	U	N	C	L	A
E	G	T	W	I	T	T
N	O	G	X	X	R	X

Solution

Now we factor in the other keyword

K	N	N	N	O	U	W
N	O	T	A	P	D	R
I	T	C	N	E	C	U
L	I	Y	G	O	T	U
I	T	T	G	R	E	I
P	T	R	T	A	H	C
E	L	U	I	N	I	T
O	Y	U	N	C	L	A
E	G	T	W	I	T	T
N	O	G	X	X	R	X

Solution

and rearrange accordingly

U	N	K	N	O	W	N
D	O	N	T	P	R	A
C	T	I	C	E	U	N
T	I	L	Y	O	U	G
E	T	I	T	R	I	G
H	T	P	R	A	C	T
I	C	E	U	N	T	I
L	Y	O	U	C	A	N
T	G	E	T	I	T	W
R	O	N	G	X	X	X

Solution

and rearrange accordingly

U	N	K	N	O	W	N
D	O	N	T	P	R	A
C	T	I	C	E	U	N
T	I	L	Y	O	U	G
E	T	I	T	R	I	G
H	T	P	R	A	C	T
I	C	E	U	N	T	I
L	Y	O	U	C	A	N
T	G	E	T	I	T	W
R	O	N	G	X	X	X

which reveals the message

> *Don't practice until you get it right; practice until you can't get it wrong.*

Hill Example

Example

The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Find the plaintext.

Hill Example

Example

The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Find the plaintext.

What do we need to do?

Hill Example

Example

The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Find the plaintext.

What do we need to do? Let's start with the inverse.

Hill Example

Example

The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Find the plaintext.

What do we need to do? Let's start with the inverse.

$$K^{-1} = \begin{bmatrix} 3 & \text{-}13 \\ \text{-}2 & 9 \end{bmatrix}$$

and

$$\begin{array}{lll} Y = 24 & I = 8 & F = 5 \\ Z = 25 & M = 12 & A = 0 \end{array}$$

Solution

Then,

$$\begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 56 & -240 \end{bmatrix} = \begin{bmatrix} 4 & 20 \end{bmatrix}$$

This gives *eu* as the start to the plaintext.

Solution

Then,

$$\begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 56 & -240 \end{bmatrix} = \begin{bmatrix} 4 & 20 \end{bmatrix}$$

This gives *eu* as the start to the plaintext.

$$\begin{bmatrix} 5 & 25 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} -35 & 160 \end{bmatrix} = \begin{bmatrix} 17 & 4 \end{bmatrix}$$

which gives re

Solution

Then,

$$\begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 56 & -240 \end{bmatrix} = \begin{bmatrix} 4 & 20 \end{bmatrix}$$

This gives *eu* as the start to the plaintext.

$$\begin{bmatrix} 5 & 25 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} -35 & 160 \end{bmatrix} = \begin{bmatrix} 17 & 4 \end{bmatrix}$$

which gives re
and finally

$$\begin{bmatrix} 12 & 0 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 36 & -156 \end{bmatrix} = \begin{bmatrix} 15 & 0 \end{bmatrix}$$

which gives ka.
Take all together, eureka the plaintext.

Affine Example

Example

The ciphertext UCR was encrypted using the affine function

$$(9x + 2) \pmod{26}$$

Find the plaintext.

Affine Example

Example

The ciphertext UCR was encrypted using the affine function

$$(9x + 2) \pmod{26}$$

Find the plaintext.

First, we find the numerical values corresponding to UCR.

$$U \mapsto 20$$
$$C \mapsto 2$$
$$R \mapsto 17$$

If $y = 9x + 2 \pmod{26}$, then we need to find y^{-1}.

Solution

$$\begin{aligned} y^{-1} &\equiv \frac{1}{9}(x-2) \pmod{26} \\ &\equiv 3(x-2) \pmod{26} \end{aligned}$$

Now we can decrypt.

Solution

$$
\begin{aligned}
y^{-1} &\equiv \frac{1}{9}(x-2) \pmod{26} \\
&\equiv 3(x-2) \pmod{26}
\end{aligned}
$$

Now we can decrypt.

$$
\begin{aligned}
U : y^{-1} &= 3(20-2) \pmod{26} \\
&\equiv 54 \pmod{26} \\
&\equiv 2 \pmod{26} \\
&\mapsto c
\end{aligned}
$$

Solution

$$\begin{aligned} y^{-1} &\equiv \frac{1}{9}(x-2)(\text{mod } 26) \\ &\equiv 3(x-2)(\text{mod } 26) \end{aligned}$$

Now we can decrypt.

$$\begin{aligned} U : y^{-1} &= 3(20-2)(\text{mod } 26) \\ &\equiv 54(\text{mod } 26) \\ &\equiv 2(\text{mod } 26) \\ &\mapsto c \end{aligned}$$

$$\begin{aligned} C : y^{-1} &= 3(2-2)(\text{mod } 26) \\ &\equiv 0(\text{mod } 26) \\ &\mapsto a \end{aligned}$$

Solution

$$
\begin{aligned}
R : y^{-1} &= 3(17 - 2) \pmod{26} \\
&\equiv 45 \pmod{26} \\
&\equiv 19 \pmod{26} \\
&\mapsto t
\end{aligned}
$$

So, the plaintext is cat.