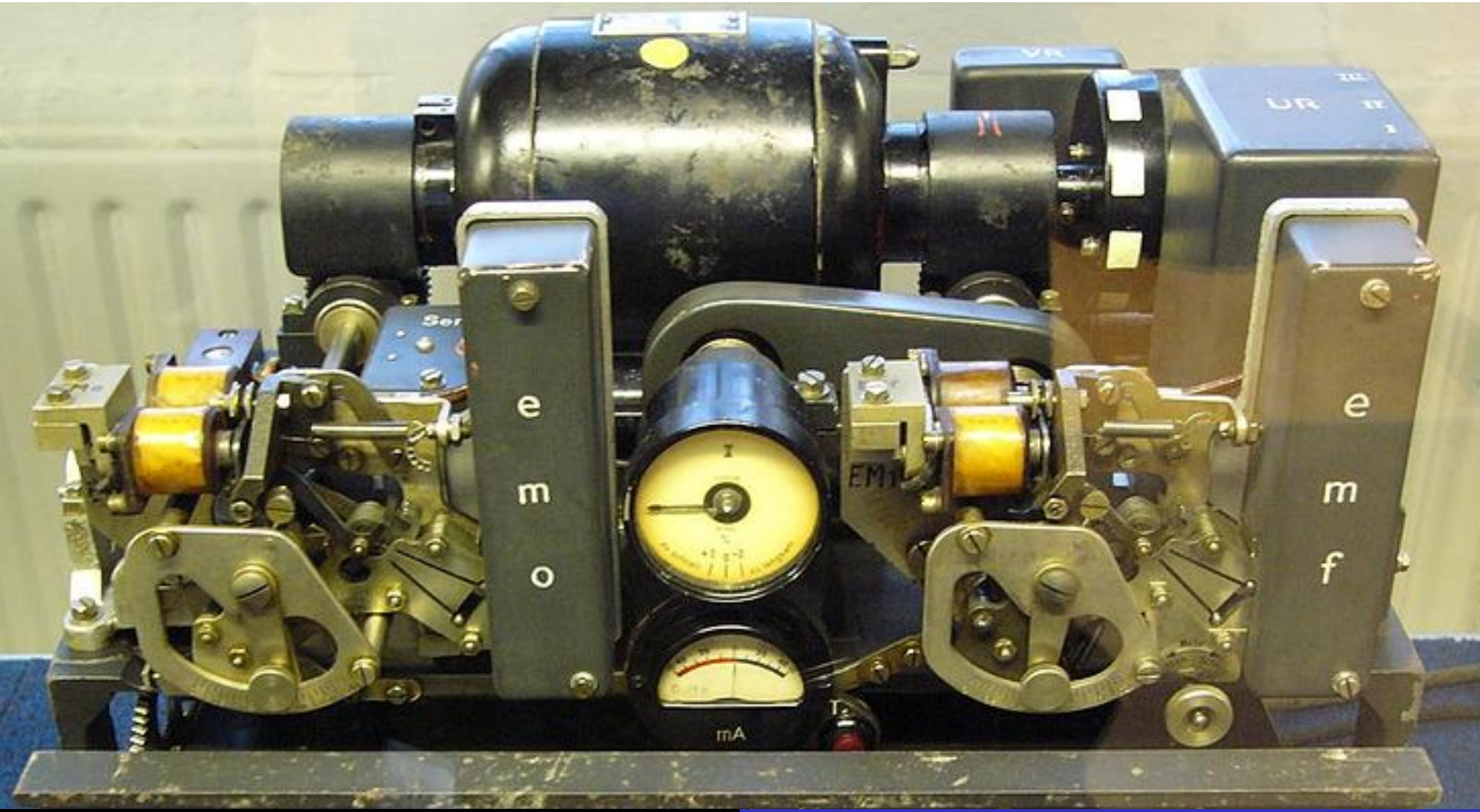
An Introduction to Cryptography

Joe Fields

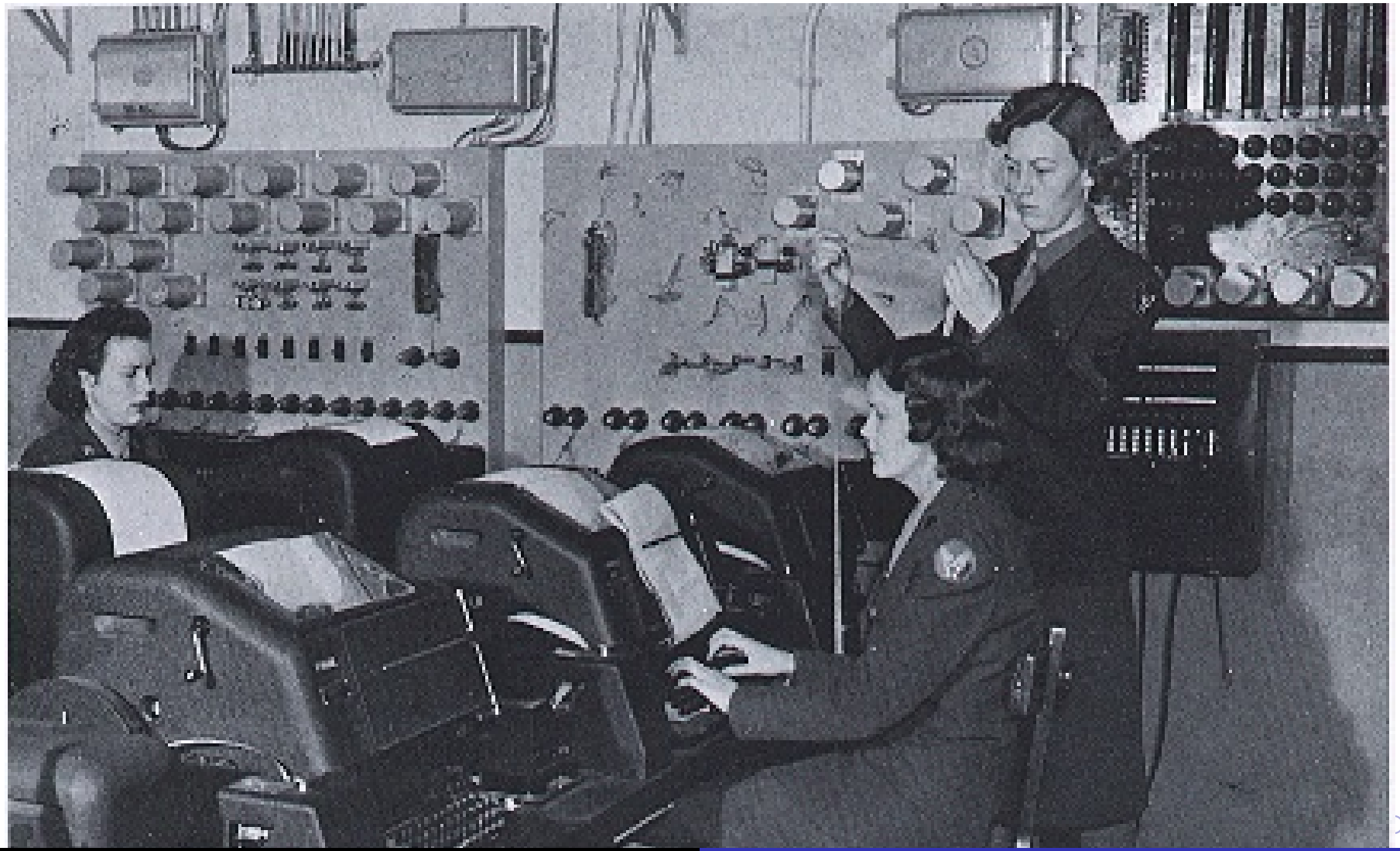
http://www.southernct.edu/~fields/

Cryptography is the study of "secret writing." This is the only branch of mathematics to be designated by the U.S. government as export-controlled. Cryptographic knowledge is considered to be "war materials!" While we won't head off into TOP SECRET territory we will have a bit of fun working out how to make (and to break) good secret codes.

the enigma



WACs



Cryptography or Cryptology?

Cryptography means “secret writing”

Cryptography or Cryptology?

Cryptography means "secret writing"
Cryptology means "the study of secrets"

Cryptography or Cryptology?

Cryptography means "secret writing"
Cryptology means "the study of secrets"
practically speaking, they are synonyms...

Cast of Characters

Alice (the sender) wants to send a message to. . .

Cast of Characters

Alice (the sender) wants to send a message to...
Bob (the recipient) but they are afraid that...

Cast of Characters

Alice (the sender) wants to send a message to. . .
Bob (the recipient) but they are afraid that. . .
Eve (the eavesdropper) will snoop on them and learn their secrets.

Components

plaintext is the message that Alice wants to send.

Components

plaintext is the message that Alice wants to send.
ciphertext is the scrambled/unreadable thing she actually sends.

Components

plaintext is the message that Alice wants to send.
ciphertext is the scrambled/unreadable thing she actually sends.
encryption is the process of converting plaintext to ciphertext.

Components

plaintext is the message that Alice wants to send.
ciphertext is the scrambled/unreadable thing she actually sends.
encryption is the process of converting plaintext to ciphertext.
decryption is the reverse process.

Components

plaintext is the message that Alice wants to send.
ciphertext is the scrambled/unreadable thing she actually sends.
encryption is the process of converting plaintext to ciphertext.
decryption is the reverse process.
cryptanalysis is what Eve has to do in order to "break the code".

A cryptosystem

The term **cryptosystem** is used to describe any systematic way to do encryption and decryption of messages.

A cryptosystem

The term **cryptosystem** is used to describe any systematic way to do encryption and decryption of messages.
Usually a **key** must also be chosen (in advance) by Alice and Bob.

A cryptosystem

The term **cryptosystem** is used to describe any systematic way to do encryption and decryption of messages.
Usually a **key** must also be chosen (in advance) by Alice and Bob.
If Eve knows the cryptosystem, she can attempt a "brute force" attack – try every possible key...

security through obscurity

People used to believe that a really Byzantine cryptosystem – for which Eve couldn't even guess what the possible keys could be – would allow Alice and Bob to communicate securely.

security through obscurity

People used to believe that a really Byzantine cryptosystem – for which Eve couldn't even guess what the possible keys could be – would allow Alice and Bob to communicate securely. Arguably, this is why Japan and Germany lost World War II.

security through obscurity

People used to believe that a really Byzantine cryptosystem – for which Eve couldn't even guess what the possible keys could be – would allow Alice and Bob to communicate securely. Arguably, this is why Japan and Germany lost World War II. Shannon's Maxim: "The enemy knows the system" (Claude Shannon (1916-2001)

cribs

If you have some idea what an encrypted message may be about, this allows you to make a list of "cribs." Cribs are words or phrases that may be part of the plaintext.

how can they decode it if they don't even know there is a message?

how can they decode it if they don't even know there is a message?

Tatoo a message on a slave's shaved head, then let their hair grow back.

how can they decode it if they don't even know there is a message?

Tatoo a message on a slave's shaved head, then let their hair grow back.
Yesterday, Oliver used a relatively easy secret message analyzer – really terrific!

how can they decode it if they don't even know there is a message?

Tatoo a message on a slave's shaved head, then let their hair grow back.
Yesterday, Oliver used a relatively easy secret message analyzer – really terrific!
It has been claimed that the Al Qaeda network hides messages in the low bits of pixels in internet porn.

Roman cryptography

Supposedly, Julius Caesar invented a simple cryptosystem: shift each letter in a message 3 units up in the alphabet:

Roman cryptography

Supposedly, Julius Caesar invented a simple cryptosystem: shift each letter in a message 3 units up in the alphabet: So,

Attack at dawn on Friday

would be encrypted as

Roman cryptography

Supposedly, Julius Caesar invented a simple cryptosystem: shift each letter in a message 3 units up in the alphabet: So,

Attack at dawn on Friday

would be encrypted as

Dwwdfn dw gdzq rq iulgdb

Activity I

Write a creative message (not too long please. . .) and encrypt it with the Caesar shift.
Trade with another group and decrypt their message.

shift ciphers

The Caesar shift is the basis of the simple cryptosystem known as the shift cipher.
The key in a shift cipher is the amount of shifting that we will do to encode a message.
(For the original Caesar shift the key is $k = 3$.)

its not *that* many possibilities

There are only 25 possible different amounts of shifting that one can do.

its not *that* many possibilities

There are only 25 possible different amounts of shifting that one can do.
We say there are 25 elements in the **keyspace**

its not *that* many possibilities

There are only 25 possible different amounts of shifting that one can do.
We say there are 25 elements in the **keyspace**
It's not really that hard to just try all the possibilities and see if any of them look intelligible.

Activity II

Pick a key – this should be a relatively small integer. Lets keep things in the range -5 to 5.
Write a creative message and encrypt it with the shift cipher using your key.
Trade with another group and decrypt their message.

too easy

To get a useful cryptosystem we will need to develop a scheme where there are many more keys!

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?
So $9+5 = 2$.

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?
So $9+5 = 2$.
Hmmmm...

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?
So $9+5 = 2$.
Hmmmm...
Suppose it's zero o'clock. (You can continue to call it 12 if you want, but 0 is really more sensible.)

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?
So $9+5 = 2$.
Hmmmm...
Suppose it's zero o'clock. (You can continue to call it 12 if you want, but 0 is really more sensible.)
What time will it be after 5 five hour time periods go by?

clock arithmetic

If it is 9:00 o'clock, what time will it be in 5 hours?
So $9+5 = 2$.
Hmmmm...
Suppose it's zero o'clock. (You can continue to call it 12 if you want, but 0 is really more sensible.)
What time will it be after 5 five hour time periods go by?
So $5 \cdot 5 = 1$.

some practice

$$11 + 2 =$$

some practice

$$11 + 2 = 1$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 =$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$
$$11 \cdot 11 =$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$
$$11 \cdot 11 = 121$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$
$$11 \cdot 11 = 121 = 1$$

some practice

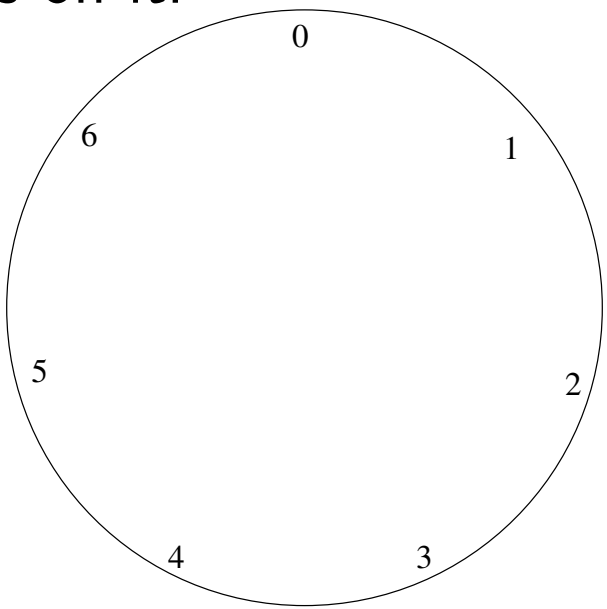
$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$
$$11 \cdot 11 = 121 = 1$$
$$6 \cdot 8 =$$

some practice

$$11 + 2 = 1$$
$$7 \cdot 5 = 35 = 36 - 1 = 11$$
$$11 \cdot 11 = 121 = 1$$
$$6 \cdot 8 = 48 = 0$$

clocks on other planets

A clock with 7 hours on it:



mod 7 operations

$4 + 5 =$

mod 7 operations

$$4 + 5 = 2$$

mod 7 operations

$4 + 5 = 2$

$6 + 4 =$

mod 7 operations

$$4 + 5 = 2$$
$$6 + 4 = 3$$

mod 7 operations

$$4 + 5 = 2$$
$$6 + 4 = 3$$
$$3 \cdot 4 =$$

mod 7 operations

$$4 + 5 = 2$$
$$6 + 4 = 3$$
$$3 \cdot 4 = 5$$

mod 7 operations

$4 + 5 = 2$

$6 + 4 = 3$

$3 \cdot 4 = 5$

Notice that the zero product property holds, since 7 is prime.

mod 26 operations and the alphabet

Each letter of the alphabet can be thought of as a number from 0 to 25. (A=0, B=1, C=2, etc.)

mod 26 operations and the alphabet

Each letter of the alphabet can be thought of as a number from 0 to 25. (A=0, B=1, C=2, etc.)
The Caesar shift can now be described mathematically:

$$x \longrightarrow x + 3 \pmod{26}$$

The general shift cipher with key k is:

$$x \longrightarrow x + k \pmod{26}$$

trouble in paradise

Sadly, arithmetic mod 26 is not so nice. Twenty-six is not prime and the zero product property fails in mod 26.

trouble in paradise

Sadly, arithmetic mod 26 is not so nice. Twenty-six is not prime and the zero product property fails in mod 26.
The problem we are worried about is whether a given operation can be inverted. Adding (i.e. doing a shift) is always invertible (just shift the other way).

trouble in paradise

Sadly, arithmetic mod 26 is not so nice. Twenty-six is not prime and the zero product property fails in mod 26.
The problem we are worried about is whether a given operation can be inverted. Adding (i.e. doing a shift) is always invertible (just shift the other way).
Multiplying, on the other hand...

trouble in paradise

Sadly, arithmetic mod 26 is not so nice. Twenty-six is not prime and the zero product property fails in mod 26.
The problem we are worried about is whether a given operation can be inverted. Adding (i.e. doing a shift) is always invertible (just shift the other way).
Multiplying, on the other hand...
The trouble arises because $26 = 2 \cdot 13$ so if we avoid numbers that have either 2 or 13 as factors life will be good.

the affine cipher

In the affine cipher we encrypt using the map

$$x \longrightarrow mx + b \pmod{26}.$$

the affine cipher

In the affine cipher we encrypt using the map

$$x \longrightarrow mx + b \pmod{26}.$$

A key is now a pair of things: m and b.

the affine cipher

In the affine cipher we encrypt using the map

$$x \longrightarrow mx + b \pmod{26}.$$

A key is now a pair of things: m and b.
The choices for m are limited to odd numbers other than 13 in the range 0 to 25. For b we can use anything in that range.

the affine cipher

In the affine cipher we encrypt using the map

$$x \longrightarrow mx + b \pmod{26}.$$

A key is now a pair of things: m and b.
The choices for m are limited to odd numbers other than 13 in the range 0 to 25. For b we can use anything in that range.
The keyspace contains $12 \cdot 26 = 312$ elements.

the affine cipher

In the affine cipher we encrypt using the map

$$x \longrightarrow mx + b \pmod{26}.$$

A key is now a pair of things: m and b.
The choices for m are limited to odd numbers other than 13 in the range 0 to 25. For b we can use anything in that range.
The keyspace contains $12 \cdot 26 = 312$ elements.
Suddenly a brute force approach is looking less enticing.

Activity III

The following message was encrypted with an affine cipher where the key was $m = 3$ and $b = 2$. I also took out spaces and punctuation (as is typical of encrypted ciphertext). What does it say?

Activity III

The following message was encrypted with an affine cipher where the key was $m = 3$ and $b = 2$. I also took out spaces and punctuation (as is typical of encrypted ciphertext). What does it say?
CBOQOXCNAPURKPWOH

duoncfzimepghvrxtjsbwlyqak

duoncfzimepghvrxtjsbwlyqak

You can make a cipher by choosing an essentially random encoding for each letter of the alphabet

duoncfzimepghvrxtjsbwlyqak

You can make a cipher by choosing an essentially random encoding for each letter of the alphabet
There are as many keys as there are possible permutations of 26 things.

duoncfzimepghvrxtjsbwlyqak

You can make a cipher by choosing an essentially random encoding for each letter of the alphabet
There are as many keys as there are possible permutations of 26 things.

$$26! = 26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 \approx 4.03 \times 10^{26}$$

duoncfzimepghvrxtjsbwlyqak

You can make a cipher by choosing an essentially random encoding for each letter of the alphabet
There are as many keys as there are possible permutations of 26 things.

$$26! = 26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 \approx 4.03 \times 10^{26}$$

Kind of a lot of those keys would be weak, in the sense that too many letters would be encrypted as themselves. But even if we restrict to only those permutations where every letter gets moved there are plenty of keys.

frequency analysis

If you have a chunk of ciphertext and one-fifth of the symbols are Q's I'll bet you can guess what letter Q represents.

frequency analysis

If you have a chunk of ciphertext and one-fifth of the symbols are Q's I'll bet you can guess what letter Q represents.
RSTLN and E

frequency analysis

If you have a chunk of ciphertext and one-fifth of the symbols are Q's I'll bet you can guess what letter Q represents.
RSTLN and E
With a sufficiently large sample of ciphertext we can use an analysis of the frequency that the symbols occur to guess (accurately) about what the decryptions of certain symbols are.

The undecipherable cipher

The undecipherable cipher

Vigenère actually invented an even better type of cipher, but through a misattribution his name is associated with this scheme, so he's just stuck with it.

The undecipherable cipher

Vigenère actually invented an even better type of cipher, but through a misattribution his name is associated with this scheme, so he's just stuck with it.
In this cipher we return to simply shifting the symbols of our plaintext up in the alphabet, but each symbol is shifted by a different amount.

The undecipherable cipher

Vigenère actually invented an even better type of cipher, but through a misattribution his name is associated with this scheme, so he's just stuck with it.
In this cipher we return to simply shifting the symbols of our plaintext up in the alphabet, but each symbol is shifted by a different amount.
Each time we run into an E it will get shifted to some other letter – but a different one each time! Frequency analysis will no longer work.

lemonlemonlemonlemonlemonlemonlem

lemonlemonlemonlemonlemonlem

The original implementations of the Vigenère cipher involved using a word or a short phrase as the key.

lemonlemonlemonlemonlemonlem

The original implementations of the Vigenère cipher involved using a word or a short phrase as the key.
The key's letters tell you how much to shift.

lemonlemonlemonlemonlemonlem

The original implementations of the Vigenère cipher involved using a word or a short phrase as the key.
The key's letters tell you how much to shift.
The key would be repeated as often as necessary so as to produce shift amounts for all of the letters in the plaintext.

really?!?

really?!?

Cryptanalysts eventually showed how to break Vigenere ciphers.

really?!?

Cryptanalysts eventually showed how to break Vigenere ciphers.
If you can figure out the length of the key you can break a Vigenere cipher into a bunch of parallel shift ciphers

really?!?

Cryptanalysts eventually showed how to break Vigenere ciphers.
If you can figure out the length of the key you can break a Vigenere cipher into a bunch of parallel shift ciphers
Each of those is easy to break seperately.

provably secure

provably secure

Even if you make the key for a Vigenere cipher so long that there are never repeats, it is possible to break them with some very high-powered statistical analysis.

provably secure

Even if you make the key for a Vigenere cipher so long that there are never repeats, it is possible to break them with some very high-powered statistical analysis.
However, if we make the key for a Vigenere-type cipher be an arbitrarily long random sequence of letters we will have secure communication.

provably secure

Even if you make the key for a Vigenere cipher so long that there are never repeats, it is possible to break them with some very high-powered statistical analysis.
However, if we make the key for a Vigenere-type cipher be an arbitrarily long random sequence of letters we will have secure communication.
This is called a “one time pad”

provably secure

Even if you make the key for a Vigenere cipher so long that there are never repeats, it is possible to break them with some very high-powered statistical analysis.
However, if we make the key for a Vigenere-type cipher be an arbitrarily long random sequence of letters we will have secure communication.
This is called a "one time pad"
There are certain places where you do not want to be caught with an arbitrarily long random sequence of letters about your person.

thanks!

Thank for coming, I hope you had fun!
http://www.nsa.gov/kids/