Codes are used to convert messages using symbols which can be communicated effectively, depending on the situation:

- Morse Code
- Braille Code
- Bar Code
- QR Code

Ciphers are used to communicate encrypted (secret) messages, like this one:

LEGAQ LASG ISRD OEPoha
MORSE CODE

International Morse Code
1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to seven dots.

Morse Tree
A branch to the left represents a dot (.)
and a branch to the right represents a dash (-).

Deciphering Morse Code

Encoded Text:

Decoded Text:

>> Online Tool
**BRAILLE CODE**

Encoded Text:

![Braaille Code Chart](image)

Decoded Text:

[Online Tool]

---

**BAR CODES**

**Anatomy of a Barcode**

![Barcode Chart](image)

- **LEFT SIDE (ODD PARITY) CODES**
  - 0: 001101, 0011011, 0010011
  - 1: 011101, 0100011
  - 2: 010101
  - 3: 011001, 0110001
  - 4: 0110001, 0101111
  - 5: 0111101, 0111011, 0101011
  - 6: 1001011
  - 7: 1010010
  - 8: 1010110
  - 9: 1101011

- **RIGHT SIDE (EVEN PARITY) CODES**
  - 0: 110011, 1100110, 1101100
  - 1: 1000010, 1011100
  - 2: 1001100, 1011100
  - 3: 1010110, 1011100
  - 4: 1011100
  - 5: 1000100
  - 6: 1001000
  - 7: 1010000
  - 8: 1011000
  - 9: 1101000


90000
CAESAR’S (SHIFT) CYPHER

A substitution cipher is a method of encryption where each letter in the alphabet is associated with a unique letter, word, or even symbols. The key to the encryption can be written in the form of a table. We can have different substitution ciphers for the same message.

Let’s shift the whole alphabet by a fixed amount to the right, say 3, and use this to encrypt the message above:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
</tbody>
</table>

MATH CIRCLES

MAGIC WHEEL

A magic wheel consists of two actual wheels, which can be rotated so that different letters in the smaller wheel correspond to the letter A of the large wheel. Ciphering using the magic wheel is done by ‘translating’ words written in the smaller wheel with the corresponding letters in the larger wheel, for example:

MATH CIRCLES
PIG PEN CYPHER

without key

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
</tr>
<tr>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
</tr>
</tbody>
</table>

with key = ‘MASON’

<table>
<thead>
<tr>
<th>M</th>
<th>A</th>
<th>S</th>
<th>O</th>
<th>N</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
</tr>
<tr>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>P</td>
<td>Q</td>
</tr>
<tr>
<td>Y</td>
<td>Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encrypting the same word gives different cyphers:

MATH =

Decipher

key = SNOWFLAKE
THE LOST SYMBOL & MAGIC SQUARE

On the newly exposed face of the pyramid, a series of sixteen characters was precisely engraved into the smooth stone.

Beside Langdon, Anderson’s mouth now gaped open, mirroring Langdon’s own shock. The security chief looked like he had just seen some kind of alien keypad.

Key 1

Key 2

Albrecht Durer’s Magic Square

DECIPHERING SUBSTITUTION CIPHERS

George Orwell
Politics and the English Language

Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot by conscious action do anything about it. Our civilization is decadent and our language — so the argument runs — must inevitably share in the general collapse...
NSA
AKA NATIONAL SECURITY AGENCY,
NO SUCH AGENCY
NEVER SAY ANYTHING

Founded in 1952 as part of Department of Defense National Intelligence Directorate
Mission to Secure Nation’s Communication while Exploiting Foreign Signals Intelligence
Largest Employer of Mathematicians in the United States

“The ability to understand the secret communications of our foreign adversaries while protecting our own communications gives our nation a unique advantage”

 Numerical values of letters for Cryptographic ciphers:

|   | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10| 11| 12| 13| 14| 15| 16| 17| 18| 19| 20| 21| 22| 23| 24| 25 |

'declare peace' = 030402110017042615040003204

See Matrices: A Secret Weapon (NSA document)

MODULAR ARITHMETIC

We first need to talk a little about modular arithmetic (also known as clock arithmetic): one fixes a positive integer \( m \) (the modulus, for real clocks \( m = 12 \)) and considers two integers \( a \) and \( b \) equal modulo \( m \) if they differ by a multiple of \( m \); in other words, \( a \) and \( b \) have the same remainder when divided by \( m \). In this case, we write \( a \equiv b \mod m \). Here are three examples:

- \( m = 12 \): We have \( 2 \equiv 14 \equiv 26 \equiv -10 \mod 12 \). (Think about hours of the day and how they would appear on a clock.)
- \( m = 2 \): Two integers are equal modulo 2 precisely if they have the same parity.
- \( m = 10 \): Two integers are equal modulo 10 precisely if they have the same last digit.

We'll concentrate on the last example, so from now on we'll do arithmetic modulo 10. Our goal is to come up with a code modulo 10; that is, we want to send a message consisting of digits, and we'd like to encode it in such a way that only our friends can decode it. In the following exercises we'll develop different codes, improving them as we move along.

Source: Stanford Math Circle: Codes, Ciphers & Secret Messages, by Matthias Beck
(1) Become familiar with addition, subtraction, and multiplication modulo 10. Compute some examples, make up a multiplication table, etc.

(2) The first code we’ll discuss goes back to Julius Caesar’s times (or so the story goes). You agree with your friend on a modulus (say, 10) and a shift parameter (say, 3). The encoding takes a digit \( d \) and moves it to \( d + 3 \mod 10 \). So let’s call the encoded digit \( e \), then

\[ e = d + 3 \mod 10 \quad \text{which is equivalent to} \quad d = e - 3 \mod 10. \]

So your friend will take the encoded digit \( e \), subtract 3 from it (modulo 10), and thus retrieve your original digit \( d \). Think about why this way of encryption is not particularly safe.

(3) We don’t have division modulo 10 in the usual sense; however, some numbers do have multiplicative inverses modulo 10. What we mean is the following: if \( a \cdot b \equiv 1 \mod 10 \) then we say that \( a \) and \( b \) are multiplicative inverses (modulo 10) of each other. Try out some numbers and see which ones have multiplicative inverses modulo 10. Based on this data, come up with a conjecture which numbers have multiplicative inverses modulo \( m \) and which don’t (where \( m \) is arbitrary). Prove your conjecture (one way to do that uses the Euclidean Algorithm).

(4) Here is our second code. Once more you agree with your friend on a modulus (say, 10) and a parameter (say, 3). The encoding takes a digit \( d \) and multiplies it by 3 modulo 10:

\[ e = 3 \cdot d \mod 10. \]

Come up with a decoding scheme. Why does it work? What happens if we replace the parameter 3 by 2? Or 6? Which parameters other than 3 could we have used? Come up with a good argument why this encryption scheme is safer than our first one. Also come up with an argument why this second scheme is still not particularly safe.

(5) Take the numbers 0, 1, 2, \ldots, 9 and multiply each of them by 3. What happens to this list of numbers? What happens if instead we multiply the list by 2? By 6? Think about how this relates to the previous exercise. Repeat this process in the general case, where we look at the numbers 0, 1, 2, \ldots, \( m - 1 \) modulo \( m \).

(6) Show that, if \( a \) has no common factor with 10 other than \( \pm 1 \) (we say that \( a \) and 10 are relatively prime), then \( a^4 \equiv 1 \mod 10 \). Can you see where the exponent 4 comes from? Come up with a similar equation for a general modulus \( m \) and think about how you could prove that equation.
MODULAR ARITHMETIC (CONT.)

(8) Now we’ll define Euler’s \(\phi\)-function: \(\phi(n)\) counts the numbers between 1 and \(n\) that are relatively prime to \(n\). Compute the first couple of values of this function: \(\phi(1), \phi(2), \phi(3), \ldots\) Find a formula for \(\phi(n)\) when \(n\) is prime. Find a formula for \(\phi(mn)\) in terms of \(\phi(m)\) and \(\phi(n)\) in the case that \(m\) and \(n\) are relatively prime. One of Euler’s theorems says that, if \(a\) is relatively prime to \(n\), then \(a^{\phi(n)} \equiv 1 \mod n\). Conclude that, if \(b \cdot c \equiv 1 \mod \phi(n)\), then \((a^b)^c \equiv a \mod n\).

(9) The previous exercise allows us to introduce the RSA cryptosystem.\(^1\) Here’s how it works: You need two prime numbers \(p\) and \(q\), compute their product \(m = pq\), find a number \(b\) that is relatively prime to \(\phi(m) = (p-1)(q-1)\), and compute an inverse \(c\) of \(b\) modulo \(\phi(m)\), i.e., \(bc \equiv 1 \mod \phi(m)\). You keep all of this private except for the numbers \(m\) and \(b\) which you make public (in particular, your friends know \(m\) and \(b\)). To send you a message \(d\), your friend encodes it as

\[ e = d^b \mod m. \]

You can decode your friend’s message by computing

\[ d = e^c \mod m. \]

Explain why this decoding works. What makes this cryptosystem safe? How could you make it safer? What would one need to break it?

\(^1\) This is precisely the RSA Encryption (named after its inventors: Ron Rivest, Adi Shamir, Leonard Adleman)

RSA ENCRYPTION

Source: [http://www.geometer.org/mathcircles/RSA.pdf](http://www.geometer.org/mathcircles/RSA.pdf)

In this example, suppose person C.S. wants to make a public key, and person L.J. wants to use that key to send C.S. a message. We will suppose that the message C.S. sends to L.J. is just a number. We assume that C.S. and L.J. have agreed on a method to encode text as numbers. Here are the steps:

1. Person C.S. selects two prime numbers. We will use \(p=23\) and \(q=41\) for this example, but keep in mind that the real numbers C.S. should use should be much larger.

2. Person C.S. multiplies \(p\) and \(q\) together to get \(m=pq = (23)(41) = 943\). The number 943 is the ‘public key’, which he tells to person L.J. (and to the rest of the world, if he wishes).

3. Person C.S. also chooses another number \(b\) which must be relatively prime to \((p-1)(q-1)\). In this case \((p-1)(q-1) = (22)(40) = 880\), so \(b=7\) is fine. \(b\) is also part of the public key, so L.J. also is told the value of \(b\).

   [So far, C.S. has chosen the private and public keys]

4. Now L.J. knows enough to decode a message to C.S.

   Suppose, for this example, that the message is the number \(d=35\).
5. L.J. calculates the value $e = d^b \pmod{m} = 35^7 \pmod{943}$.

6. $35^7 = 64339296875$ and $64339296875 \equiv 545 \pmod{943}$. The number $e=545$ is the encoding that L.J. sends to C.S.

7. Now C.S. wants to decode 545. To do so, he needs to find a number $c$ such that $bc = 1 \pmod{(p-1)(q-1)}$, or, in this case, such that $7c = 1 \pmod{880}$. A solution is $c=503$, since $7*503 = 3521 = 4*880 + 1 = 1 \pmod{880}$.

8. To find the decoding, C.S. must calculate $e^c \pmod{m} = 545^503 \pmod{943}$. This looks like it will be a horrible calculation, and at first it seems like it is, but notice that $503 = 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1$ (this is just the binari expansion of 503). So this means

\[
545^{503} = 545^{256} \cdot 545^{128} \cdot 545^{64} \cdot 545^{32} \cdot 545^{16} \cdot 545^{8} \cdot 545^{4} \cdot 545^{2} \cdot 545^{1}.\]

Since we only care about the result $\pmod{943}$, we can calculate all partial results in that modulus, and by repeated squaring of 545, we can get all the exponents that are powers of 2. For example, $545^2 \pmod{943} = 545 \cdot 545 = 297025 \pmod{943}$. The squaring again: $545^4 \pmod{943} = (545^2)^2 \pmod{943} = 923 \cdot 923 = 8511929 \pmod{943} = 400$, and so on. We obtain the following table:

<table>
<thead>
<tr>
<th>$545^1 \pmod{943}$</th>
<th>$= 545$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$545^2 \pmod{943}$</td>
<td>$= 923$</td>
</tr>
<tr>
<td>$545^4 \pmod{943}$</td>
<td>$= 400$</td>
</tr>
<tr>
<td>$545^8 \pmod{943}$</td>
<td>$= 633$</td>
</tr>
<tr>
<td>$545^{16} \pmod{943}$</td>
<td>$= 857$</td>
</tr>
<tr>
<td>$545^{32} \pmod{943}$</td>
<td>$= 795$</td>
</tr>
<tr>
<td>$545^{64} \pmod{943}$</td>
<td>$= 215$</td>
</tr>
<tr>
<td>$545^{128} \pmod{943}$</td>
<td>$= 18$</td>
</tr>
<tr>
<td>$545^{256} \pmod{943}$</td>
<td>$= 324$</td>
</tr>
</tbody>
</table>

So the result we want is

\[
545^{503} \pmod{943} = 324 \cdot 18 \cdot 215 \cdot 795 \cdot 857 \cdot 400 \cdot 923 \cdot 545 \pmod{943} = 35.
\]

which is exactly the original number that L.J. chose to be encoded.
RSA EXERCISE

Can you do this type of encryption yourself?
[Choose some small numbers, and you may want to use a scientific calculator]

Your private key

\[ p = \quad q = \] 

Your public key

\[ m = pq = \quad b = \quad [\text{must be relatively prime with } (p-1)(q-1)=] \]

Original number (to be encoded): \[ d = \]

Encoding: \[ e = d^b \pmod{m} = \]

Decoding: First find a number \( c \) such that \( bc = 1 \pmod{(p-1)(q-1)} \)
and write its binary expansion

\[ c = \]

Compute \[ d = e^c \pmod{m} = \]