Encryption
Certain personal information is often sent to others. The means of sending the information is often not secure. This creates the need to encrypt the information; that is, the information needs to be recorded in such a way that somebody who intercepts the information cannot figure out what is the information, while the intended recipient should be able to see what it is.
A good example of the need for encryption is internet banking or purchasing. For example, if you buy something on amazon.com, you will enter your credit card. When you click buy, the information is transmitted across the internet, which is not a secure environment. By using a secure webpage, the information is encrypted with some method.
Today we will consider some historical methods of encryption and some extensions. Thursday we will discuss a method, discovered in 1977, which is simple to use and appears to be very secure in spite of its ease and speed of computers.
Encryption was used heavily during the two world wars. The defeat of the Nazis in WWII was greatly sped up by the allies breaking Nazi codes in the last couple years of the war.

Thanks to the use of Native American languages, the allies were able to keep their transmissions from being deciphered during each of the wars.

The work of Native Americans in the war effort was documented by the 2002 film "Windtalkers."
The Caesar Cipher

Perhaps the first recorded use of encryption came from the time of Caesar. Back then messages were written down and carried from person to person by a runner. If the runner was captured, how could they keep the message secret?
One method used then is now referred to as the **Caesar cipher**. The word cipher refers to a process (or algorithm) for taking information and making it unreadable to anybody but the intended recipient.

The Caesar cipher method takes a message and shifts each letter a certain amount.
For example, suppose we shift each letter three places to the right. Each letter is replaced by the one immediately below it in the table below.

<table>
<thead>
<tr>
<th>original</th>
<th>ABCDEFGHIJKLMNOPQRSTUVWXYZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>cipher</td>
<td>DEFGHIJKLMNOPQRSTUVWXYZABC</td>
</tr>
</tbody>
</table>
For example, to encrypt with this method:

\[
\text{send help now}
\]

you would write it as

\[
\text{vhqg khos qrz}
\]

If somebody intercepted the encrypted message, they would not know what is the original message.
When the desired recipient gets the encrypted message, they would use the encryption table in reverse. For each letter in the message, they would find the letter in the bottom row. They would replace a letter by the corresponding letter in the top row.

This process is called decrypting.
The Caesar cipher method has 25 variants: we can shift the letter A to any other letter of the alphabet. Note that a shift to the left can be accomplished by an appropriate shift to the right. For example, shifting to the left by 1 letter is the same as shifting to the right by 25 letters:

| original | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| cipher   | ZABCDEFGHIJKLMNOPQRSTUVWXYZ |
Another way to think about decrypting, or going backwards, is that if you shift 3 to the right to encrypt, you shift 3 to the left (= 23 to the right) to decrypt.

So, decrypting and encrypting use the same method in the Caesar cipher.
Security of a Cipher and Decrypting

How secure is the Caesar cipher? In other words, could an interceptor steal a message and figure out what the message should be?
A mark of a good encryption method is that it should be very difficult for messages to be deciphered.

We can talk about security and how to decrypt at the same time.
For example, suppose that the message

\textbf{drsc sc k docd}

is received. If we know that a Caesar cipher is used, then with some trial and error, we can figure out that the intended message is

\textbf{this is a test}

The spreadsheet TammyAndRex.xls available on the course website can make doing this simple.
In order for Caesar cipher to be used effectively, nobody but the intended recipient should know that the method is being used. If you know that this method is being used, it is fairly simple to decipher a message. We illustrated this in the example on the previous slide.
Encryption via Remainder Arithmetic

By thinking more mathematically, we can understand better the Caesar cipher, and come up with other encryption methods. All the methods we will discuss involve the idea of remainder arithmetic, which also arose in our discussion of the Hamming code.
mod 26 arithmetic

To discuss the Caesar cipher, we will use mod 26 arithmetic. To use this arithmetic, we only use the numbers 0, 1, 2, ..., 25.

To add or multiply two of these mod 26, first do the original arithmetic, then keep the remainder after dividing the result by 26.
For example, in mod 26, if we want 20 + 11, we first compute the ordinary sum, which gives 31. We then divide 31 into 26, getting 1 with a remainder of 5. We then have

\[ 20 + 11 = 5 \text{ in mod } 26 \]

Similarly,

\[ 5 \times 6 = 4 \text{ in mod } 26 \]

because 30 divided by 26 leaves a remainder of 4.
An alternative way to think about this arithmetic is to do the ordinary arithmetic, and then add or subtract 26 enough times in order to get a number between 0 and 25.

For example, to see that

$$7 \times 7 = 23 \text{ in mod 26},$$

you first compute $7 \times 7 = 49$ in ordinary arithmetic. Then subtract 26 to get 23.
Similarly,

\[ 8 \times 8 = 12 \text{ in mod } 26 \]

since in ordinary arithmetic, \( 8 \times 8 = 64 \).
Subtracting 26 gives \( 64 - 26 = 38 \). Subtracting
again gives \( 38 - 26 = 12 \).
Interpreting the Caesar Cipher in Mod 26

If we consider the shift by 3 letter cipher, then we can do this numerically as follows. First, we assign each letter a number in mod 26. For example, we could assign \( a = 0, \ b = 1, \ c = 2, \) and so on, until we have \( z = 25. \)
To encrypt, we would replace any letter by the corresponding letter obtained by adding by 3 mod 26.

For example, to encrypt \( y \), we would replace \( y \) by 24, then add 3 mod 26. Since

\[
24 + 3 = 1 \mod 26,
\]

we would then replace \( y \) by \( b \).
In other words, to encrypt any letter, take its numerical value, and add 3 in mod 26. Taking the corresponding letter would then give the encrypted letter.

Spreadsheets can handle mod arithmetic very easily. Excel uses the function mod. If you enter =mod(62, 26), the spreadsheet determines what number mod 26 represents 62 (which is 10).
For example, the message

you are here

would be represented numerically by

24 14 21 0 17 4 7 4 17 4

Adding 3 to each number, mod 26, results in the encrypted message

1 17 24 3 20 7 10 7 20 7

which corresponds to the text

bry duh khuh
Using arithmetic allows other encryption methods. For example, instead of adding a fixed number in mod 26, we could multiply by a fixed number.

In the Tammy and Rex spreadsheet, The Tammy cipher, which is the same as the Caesar cipher, uses adding by a fixed number mod 26.

Decrypting the Tammy cipher is done by subtracting, rather than adding, the fixed number mod 26.
The Rex Cipher multiplies by a fixed number mod 26.

In the Tammy Cipher, the encryption key \( K \) for Tammy means, since \( K \) is assigned the number 10, to add 10 to each number mod 26.

For the Rex Cipher, the encryption key represents the fixed number by which we multiply. For example, the key \( D \), which stands for 3, means multiply each number by 3 mod 26.
In Rex D, to encrypt $W$, we would first replace $W$ by 22, then multiply by 3 in mod 26. We first multiply $22 \times 3 = 66$. We then subtract 26 until we get a number between 0 and 25. Since $66 - 26 = 40$ and $40 - 26 = 14$, we would then replace $W$ by the letter for 14, which is $O$. 
One serious problem with the Caesar (= Tammy) and Rex ciphers is that if the method being used is discovered, even if the specific encryption key is not known, then it is very easy to decipher messages.

Moreover, any encryption method that involves rearranging letters can be deciphered given enough text, by knowing something about which letters are more commonly used than others, and which letters make up short words.
Cryptograms are (or were) frequently given in newspapers next to the crossword puzzles. Often a line of text, perhaps with a hint, was all that it takes to decipher the text.

They can be built from any rearrangement of letters. No specific method is necessarily used in a given cryptogram.
Therefore, in order to have a truly useful method of encrypting data, a more sophisticated method of encryption is needed. We will talk about one such example, the RSA system, on Thursday.