Date Shift Cipher

Overview: The Date Shift cipher is a much harder code to break than the simpler Shift Cipher. This is because the Date Shift number key varies from letter to letter, and also because it's *polyalphabetic* (this means that a number or letter can represent multiple letters).

Materials

- Pencil
- Paper

Activity: First, you need a date. I like to use the date that the message was sent. Suppose we pick a date: May 12, 1996. Let's figure out the shift key based on the date: change the date into a numerical date like this: 05/12/96. Now erase the slashes and write all the numbers together like this: 051296. That's our shift key. Let me show you how to use it.

I have a message to code: "LOOK UNDER DESK"

To encode it, write the date shift key 051296 above the message. If the message is longer than the key, just repeat the number sequence of the key to fit the message.

0 5 1 2 9 6 0 5 1 2 9 6 0

L O O K U N D E R D E S K

The numbers above the letters represent the shift key for that letter. All letters are shifted by their own personal shift key, like this:

L is not shifted at all, since its shift number is zero, so L = L.

The first O will be shifted 5, so it becomes a T.

The next O will be shifted once to become a P.

K is shifted by 2 to become M.

U is shifted 9 times which becomes a D. (You'll have to start at A after you get to Z to make this work.)

When you shift all the letters and group them in groups of 5, your message becomes:

LTPMD SDJSF NYK

Fill in the last few spaces with holders: ZQ.

LTPMD SDJSF NYKZQ

To decode the message, make sure you give your friend the date shift key, or it will be nearly impossible to break this code (even if they're good at breaking substitution ciphers).

Here's how to decode the message:

0 5 1 2 9 6 0 5 1 2 9 6 0 5 1

L T P M D S D J S F N Y K Z Q

Now shift each of the letters backward:

L is not shifted, so it stays as L.

T is shifted 5 times backward to become an O.

P is shifted back one space to become an O. (Notice that both T and P represent O. That's why regular substation cipher decoding doesn't work!)

Continue shifting back to decode and find the original message: LOOK UNDER DESK (Ignore the last "ZQ" term.)

What do you think about the Date Shift cipher? The possibilities for numerical keys are endless. You can use the date you're sending the message, birth dates, phone numbers, and more! Just remember to start decoding by writing the key numbers over the top of the encoded cipher. And *always* makes sure the decoder has the correct numerical key!

Now it's your turn! Work out the exercises below. (You'll find answers at the back of this book.)

Exercises

1. Which kind of key is used in date-shift ciphers?
2. In which direction is the cipher shifted when decoding?
3. How do you describe a cipher where a specific alphabetical letter represents more than one letter?

What would be the date shift key codes for the following?

4. April 4th 1998 (Don't forget that the key needs six digits! Use "04" for the date.)
5. Jan. 28th 2012
6. Nov. 30th 2011

Encode the following:

7. COME TO MY HOME : March 16th 1999
8. THEY HAVE JUST LEFT : June 1st 2001

What are the original messages? (These messages were sent on July 16th 1992)

9. GLBZC GNHNQ
10. MLFZT GAATO GRMZQ