

**Cryptanalysis of shift ciphers**

**Overview.** This exercise introduces the use of frequency histograms to break shift ciphers.

**Things to do.**

1. Obtain some blank frequency histograms, some ordinary English text, and a copy of the “Shift Ciphers” cryptogram sheet.
2. Record about 200 consecutive letters (about 40 words) from the ordinary text in one of the histograms. Compare your histogram with the supplied double-length histogram.
3. Pick one of the cryptograms on the Shift Ciphers sheet and fill in a frequency histogram using the first 200 letters (that is, the first 40 groups) in the ciphertext.
4. (Optional) Convert the histogram to a frequency table by dividing the number in the histogram by 200. Fill in the frequency table below. Round to two decimal places.

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

Do you get one letter with a frequency of about 12% and three others with a frequency of about 9%?

5. Slide the double-length standard frequency histogram along the histogram you made in step 3. The position that gives the best match tells you the key to the shift cipher.
6. Decrypt at least the first line or so of your ciphertext. Use Excel if you want to, or your cipher disk.