Math 135 (Summer 2006)
Monoalphabetic Substitutions

A **monoalphabetic substitution** is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.

Example: An affine cipher $E(x) = (ax + b) \bmod 26$ is an example of a monoalphabetic substitution.

There are other ways to "generate" a monoalphabetic substitution.

Alphabet Mixing via a Keyword

A **keyword** or **key phrase** can be used to mix the letters to generate the cipher alphabet.

Example: If the keyword is `ANDREW DICKSON WHITE`, then the cipher alphabet is given by

plain	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
cipher	A	N	D	R	E	W	I	C	K	S	O	H	T	B	F	G	J	L	M	P	Q	U	V	X	Y	Z

Do you think it is a problem that there are 5 **collisions** (a plaintext letter being substituted for itself) in this substitution? (Answer: It depends.)

Perhaps a better keyword is `EZRA CORNELL`:

plain	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
cipher	E	Z	R	A	C	O	N	L	B	D	F	G	H	I	J	K	M	P	Q	S	T	U	V	W	X	Y

Note that neither of these substitutions are generated by an affine cipher.

Alphabet Mixing via a Columnar Transposition

The letters from the keyword form the headings of the columns, and the remaining letters of the alphabet fill in order in the rows below. Mixing is achieved by transcribing columns.

Example: If the keyword is `CORNELL`, then write

C	O	R	N	E	L
A	B	D	F	G	H
I	J	K	M	P	Q
S	T	U	V	W	X
Y	Z				

so that transcribing columns left-to-right gives the substitution

plain	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
cipher	C	A	I	S	Y	O	B	J	T	Z	R	D	K	U	N	F	M	V	E	G	P	W	L	H	Q	X

For instance, `FAR ABOVE CAYUGA'S WATERS` is enciphered as `OCVCA NWYIC QPBCE LCGYE`.

Note that this substitution is also *not* generated by an affine cipher.