Design Example

Designing a Program

- Substitution ciphers exchange each plaintext letter with another (letter or symbol)
- Start with easiest- Caesar cipher
  - Rotation cipher, shift all letters a fixed amount
  - A becomes B, U becomes V for shift of 1
- Need
  - Input- read in plaintext and shift
    - Verify all are alphabetic characters
  - Shift- create the ciphertext
  - Output- produce ciphertext to screen or file

Deciphering?

- We need to decipher the message too!
- Easy!
  - Modify the encrypt function to subtract the shift rather than add it
- Add and subtract the shift??
  - char data type is numeric
  - Add the shift value to the char value and take modulus 26
  - Or subtract it

Are we all done?

- Maybe
  - Caesar is too simple
  - Only need to check 25 shifts
  - Why not 26?
- Use a keyed ciphtertext alphabet with a shift
- Key = beavers (skip repeated letters) include a blank character & shift 4 we get:

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

Changes?

- Modify input function
  - Add 2D array to hold plaintext alphabet
  - Use shift and key to fill the other row
  - For each P value output the corresponding C value
- To decipher?
  - Build the 2D array and fill it
  - For each C value output the corresponding P value
- May now need a menu and other modifications to input function

Changes?

- Due to retaining blanks cryptanalysis is easy
  - Cipher; WXJX WXA
  - Likely plaintext; that the
- Easy fix!
- Modify cipher array to not include blanks
- Still requires modification to encryption and input functions

Changes?

- Use multiple cipher alphabets

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

Changes?

- New encrypt and decrypt functions using a 2D array, that's much bigger 27R x 27C
- Revised input function
  - Simpler since you only need the plaintext and the keyword, there's no shift
- Really need a menu if you haven't added one
- Maybe split the encryption/decription functions into 2 groups?
  - Monoalphabetic
  - Polyalphabetic

Is there more?

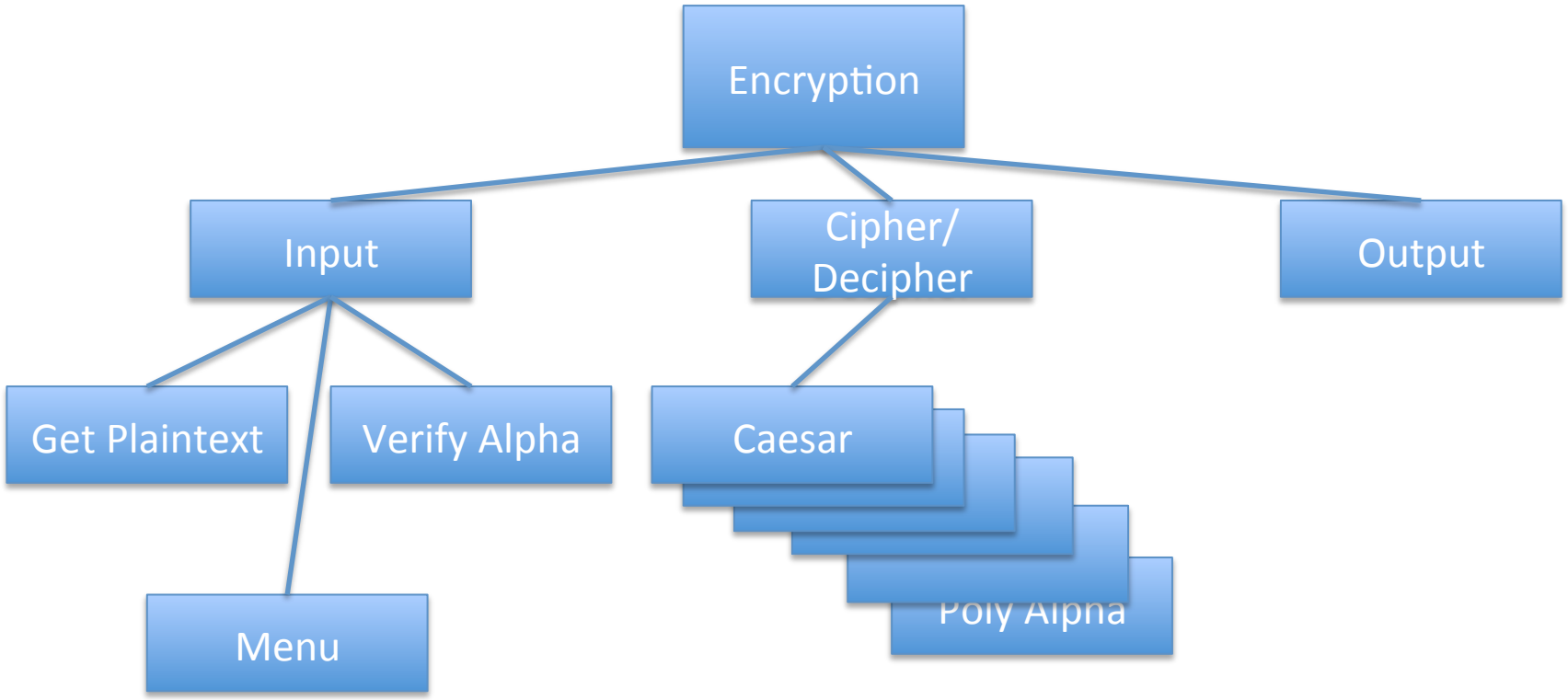
- Yes , add more keyed alphabets
  - Replace straight ciphertext alphabets (rows 2-27)
  - Add key to the key index (i.e. the first column)
  - Replace the plaintext alphabet (first row)
- Left as an exercise for the user
- Changes involve building the table so internal to the encrypt/decrypt function

Changes?

- Use multiple keyed cipher alphabets

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

Where Are We At?



This is just a decomposition of operations to perform. We haven't addressed how the software will be organized. That's the next step.
There is rarely just one "correct" decomposition.

Important Points

- Decomposition limits the changes required to the program to specific places
- If one part gets too large or complicated then split it further
- So far it is paradigm independent, i.e. neither procedural or object oriented
- Next step is to convert it to modules or classes

Note

- All the cipher systems used in this exam are “real world” pen and paper cipher systems.

Caesar	Also called rotation
Simple Substitution with word divisions	Also called an aristocrat
Simple Substitution with out word divisions	Also called a patristocrat
Polyalphabetic	Also called the Vigenère
Polyalphabetic with changes to order of the alphabets	Also called variant, Beaufort, and others
Polyalphabetic with keyed alphabets of all combinations	Also called quagmire I, II, III, and IV.

Note (continued)

- The Vigenère cipher was developed in the 16th century.
- It was considered unbreakable for nearly 300 years.
- The application of mathematical and statistical analysis finally allowed breaking of the “unbreakable cipher”.
- As a result the other variations were added to regain the security of the encrypted messages.
- We have not discussed transposition ciphers which require entirely different techniques as you adjust the order of the letters, you don’t change them.
- Nor have we discussed combination ciphers that do both.