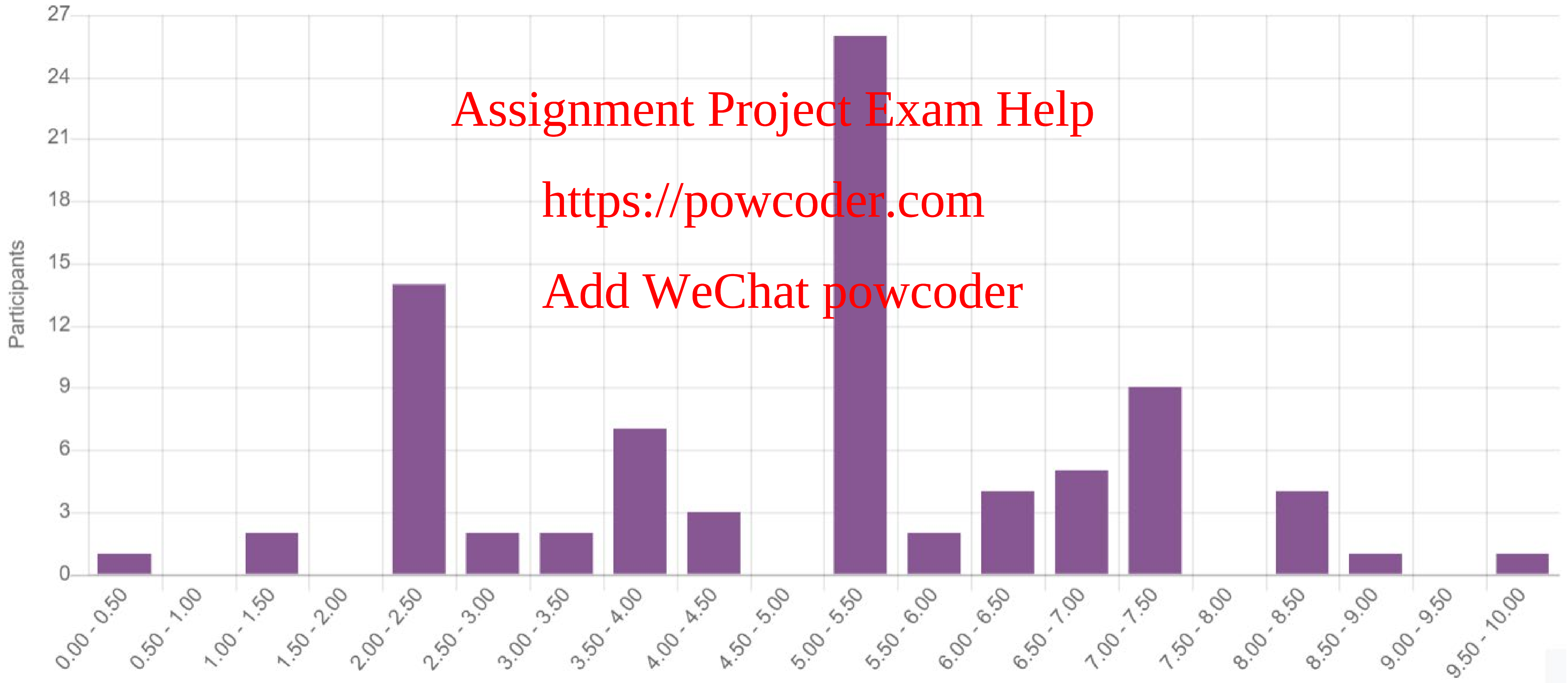
Quiz 6 - statistics

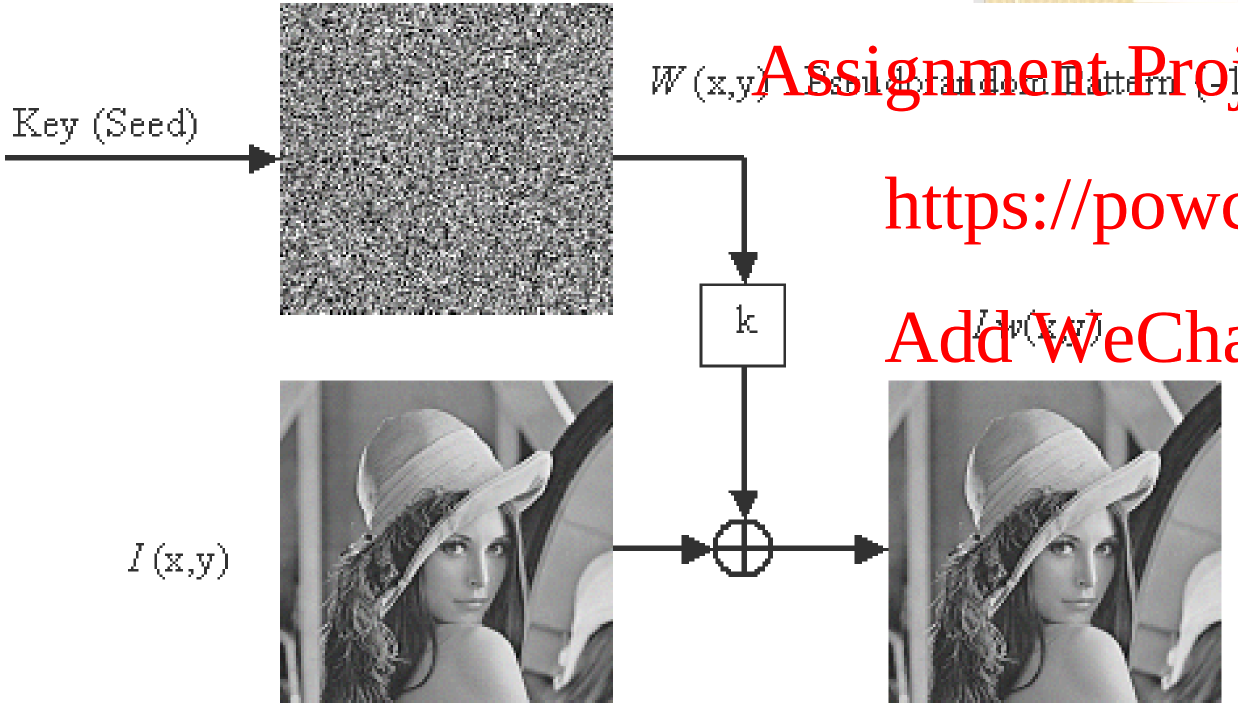
# of participants: 82 / 100
average: 5.80 / 10



Watermark / Entropy Question

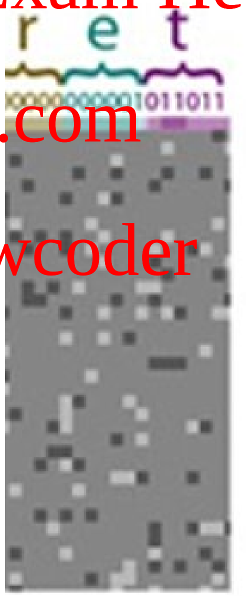
class average: 0.61 / 2 [30.5%]

The entropy or average information of an image is a measure of the degree of randomness in the image.



$$Iw(x,y) = I(x,y) + k*W(x,y)$$

Is 'random' choice of pixels an ideal approach to information hiding in an image ???



Should not 'mess up' pixel values in areas of 'low entropy'.

at is a better place to hide secret bits:

- same-color background
- part of image with lots of detail ???

In order to exchange confidential messages with each other, Alice and Bob use an encryption system/software in which every new message is encrypted <u>using a different symmetric key</u>.

Trudy is able to capture/sniff these messages, and she also wants to be able to decrypt them.

If Trudy is in the position to conduct (only) one of the following types of attacks on the given system, which one should she choose to conduct in order to achieve her objective in the shortest period of time?

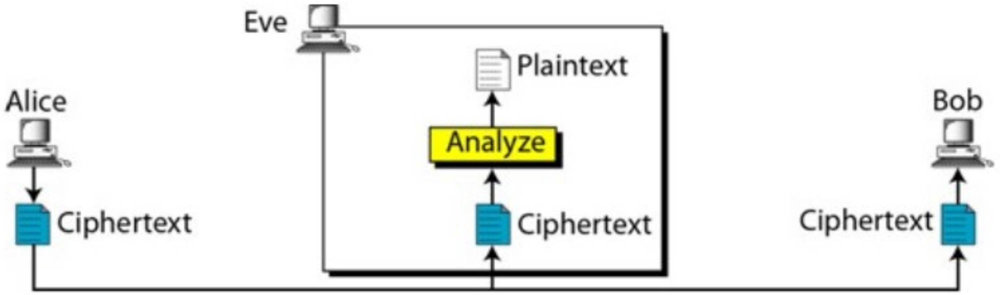
[✓ 1) ciphertext only]

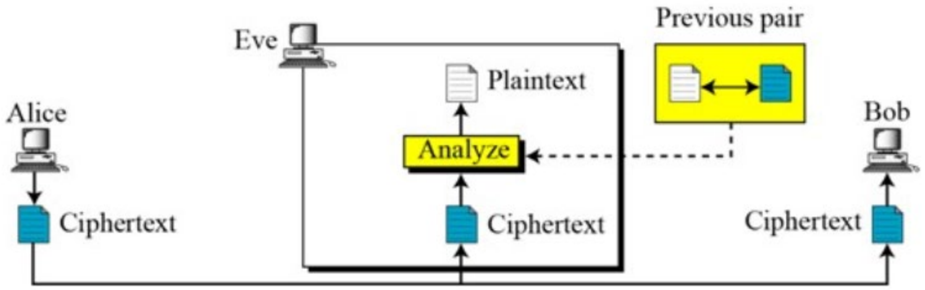
2) chosen plaintext

3) chosen ciphertext

4) chosen text

Appropriate only in systems where the same key is used multiple times …





You have captured a ciphertext that was exchanged between Alice and Bob.
You have also learned that:

- The given ciphertext is produced using Vigenere cipher;
- The encryption key used is a 5-character sequence that starts and ends with letter ‘A’.
- The plaintext corresponding to the captured ciphertext starts with word ‘HELLO’.

If the first word of the captured ciphertext is ‘HFNMO’, what was the encryption key used by Alice and Bob?

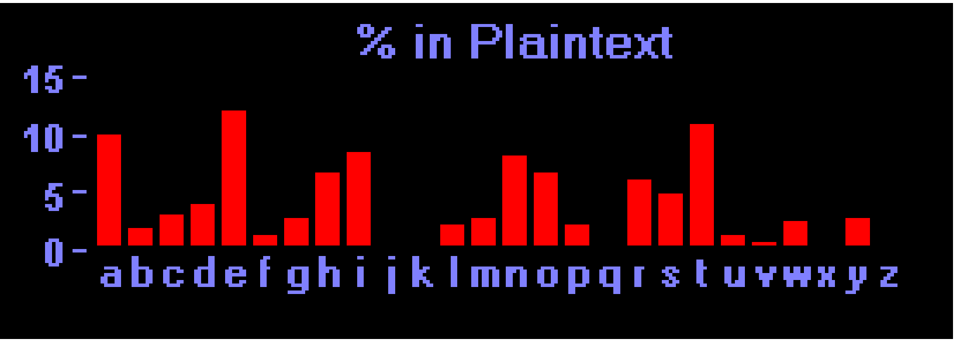
Plaintext: H E L L O
Key: A B C B A
Ciphertext: H F N M O

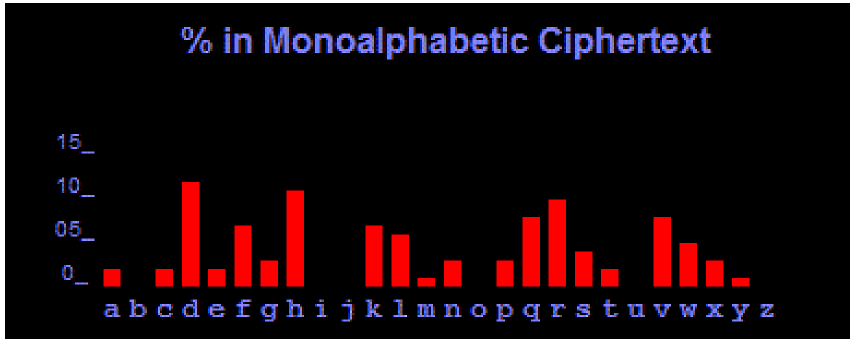
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

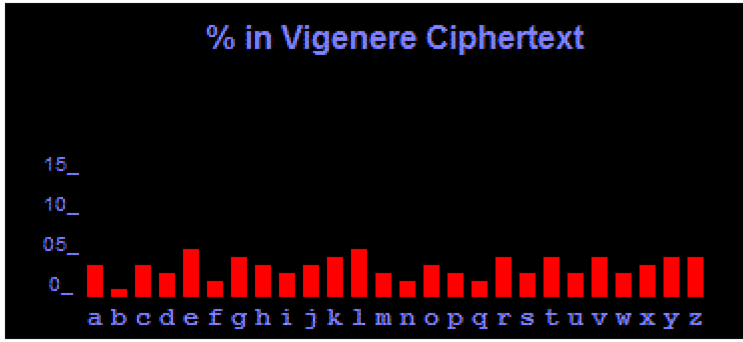
In which of the following situations the use of Frequency Analysis would be an appropriate approach to finding the plaintext?

1) a short plaintext was encrypted using a simple substitution cipher (e.g., Caesar)
2) [✓ a long plaintext was encrypted using a simple substitution cipher (e.g., Caesar)]
3) a short plaintext was encrypted using a complex substitution cipher (e.g., Vigenere)
4) a long plaintext was encrypted using a complex substitution cipher (e.g., Vigenere)

Frequency Analysis is only appropriate for plaintexts/ciphertexts that contain a significant number of characters/letters, and their distribution/histogram matches the overall character/letter distribution of the respective language …


% in Plaintext


% in Monoalphabetic Ciphertext


% in Vigenere Ciphertext

In class we have discussed the operation of a symmetric-encryption system with a Key Distribution Center (KDC).

Consider such a system with 6 users, as shown in the below figure. Currently, in this system, Alice is in the process of exchanging confidential messages with Bob, and Ted is in the process of exchanging confidential messages with Betsy.

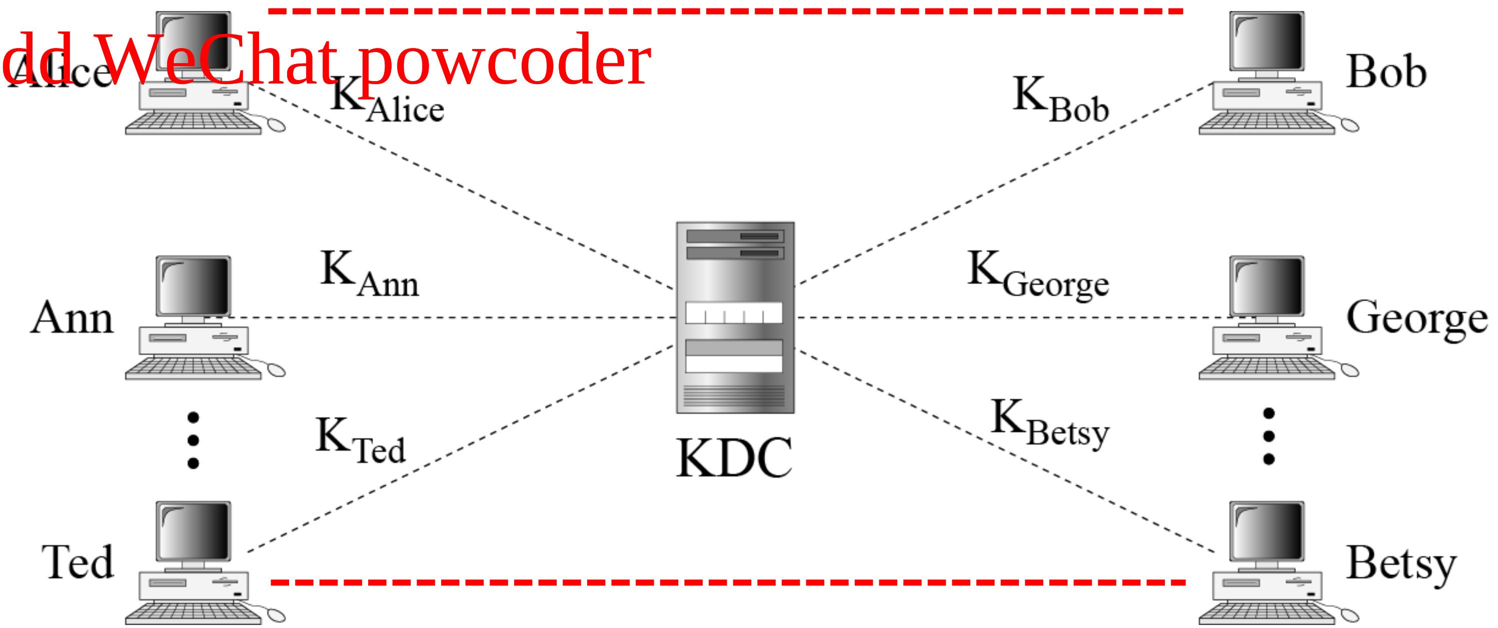
What is the overall number of symmetric keys that the KDC of this system needs to know/store at this particular point in time? (I.e., what is the number of symmetric keys in use?)

1) 2

2) 4

3) 6

[✓ 4) 8]


Alice
K_{Alice}
K_{Bob}
Bob
Ann
K_{Ann}
K_{George}
George
K_{Ted}
KDC
K_{Betsy}
Ted
Betsy