MATH 4161 Mathematics of Cryptography **Assignment 5**

ASSIGNMENT JOE TRAN

Question 1. Given the ciphertext: 102-85-119-80-16-86-119-92-82-107-20 82-68 55-42-12-67-45-92-101-102-20-80 82-69 102-68 92-29-12 36-90-78-94-16-78-43 21-27 18-82-27-12'91 121-35-19-82-86-57 99-40-92-38-119-76-92-102-21-86-39, determine the plaintext and the key.

Solution. Since we our largest value in the given ciphertext is 121, then at most, we would have 5 rows in our homophonic table. We will first have a look at the punctuation. Since we have '91, there are only a few common apostrophes that we can have here: 'd, 't, or 's.

We claim that the contraction is 's, i.e. S is 91. Then we have the table for the 4th row given as:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
99	100	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98

So now filling out what we have: 102-M-119-G-16-N-119-T-I-107-20 I-68 55-42-12-67-45-T-101-102-20-G I-69 102-68 T-29-12 36-R-E-V-16-E-43 21-27 18-I-27-12'S 121-35-19-I-N-57 A-40-T-38-119-C-T-102-21-N-39.

Now let us have a look at the two-letter words. Namely, I-68 and I-69. The only two words that can make sense in this situation is IS and IT, and since S is before T, we claim that S is 68 and T is 69. Then with this information, our third row becomes

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75

Then with the information above, we now have: 102-M-119-G-16-N-119-T-I-107-20 I-S E-42-12-R-45-T-101-102-20-G I-T 102-S T-29-12 36-R-E-V-16-E-43 21-27 18-I-27-12'S 121-35-19-I-N-G A-40-T-38-119-C-T-102-21-N-39.

Now let us have a look at the next two letter word, namely 102-S. Now the only one letter that can come to mind is I. If this were the case, then I would be 102 for the 5th row, and so

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
119	120	121	122	123	124	125	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118

Then with the information above, we now have: I-M-A-G-16-N-A-T-I-O-20 I-S E-42-12-R-45-T-H-I-20-G I-T I-S T-29-12 36-R-E-V-16-E-43 21-27 18-I-27-12'S C-35-19-I-N-G A-40-T-38-A-C-T-I-21-N-39.

Now let us have a look at the first word I-M-A-G-16-N-A-T-I-O-20. There is only one word in which we can spell at this point is IMAGINATION. Therefore, I would be 16 in row 1.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7

Then with the information above, we now have: I-M-A-G-I-N-A-T-I-O-N I-S E-42-E-R-45-T-H-I-N-G I-T I-S T-29-E 36-R-E-V-I-E-43 O-27 L-I-27-E'S C-35-M-I-N-G A-40-T-38-A-C-T-I-O-N-39.

Finally, let us have a look at the two letter word O-27. The only acceptable word in this case would be OF, so we claim that F is 27. If this was the case, then

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
47	48	49	50	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

Finally, completing the sentence: I-M-A-G-I-N-A-T-I-O-N I-S E-V-E-R-Y-T-H-I-N-G I-T I-S T-H-E P-R-E-V-I-E-W O-F L-I-F-E'S C-O-M-I-N-G A-T-T-R-A-C-T-I-O-N-S.

Therefore, the plaintext is: *Imagination is everything it is the preview of life's coming attraction.* Combining the above tables, we have the homophonic substitution table given by

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7
47	48	49	50	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
99	100	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98
119	120	121	122	123	124	125	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118

So the keyword is *TEACH*.