Many Time Pad

Ý tưởng:

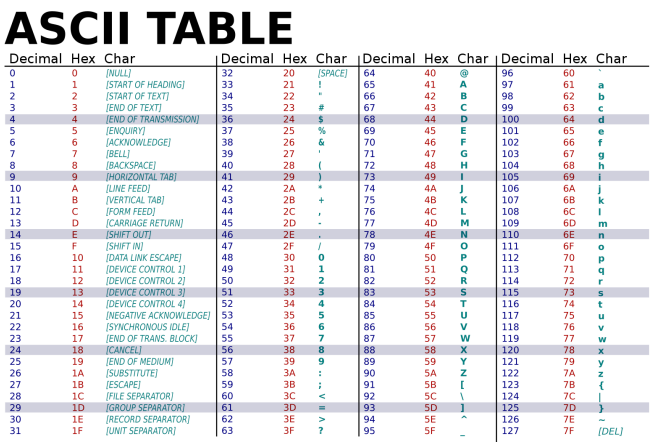
- Với khoá k, xét các kí tự x_1, x_2 được mã hoá thành các kí tự y_1, y_2

  $y_1 = x_1 \oplus k,\ y_2 = x_2 \oplus k$

  Ta có,

  $$y_1 \oplus y_2 = (x_1 \oplus k) \oplus (x_2 \oplus k) = (x_1 \oplus k) \oplus (k \oplus x_2) = x_1 \oplus (k \oplus k) \oplus x_2) = x_1 \oplus x_2$$

- Ngoài ra việc XOR một kí tự ASCII với space sẽ đổi chỗ kí tự các cột 1-2, 3-4 tương ứng trong bảng sau



ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Nguồn: wikipedia.org

Ví dụ: ‘A’ XOR ‘ ‘ = ‘a’

Bước 1:

Với mỗi ciphertext ta sử dụng phép XOR ciphertext đó với tất cả các ciphertext còn lại thu được danh sách list_xored bao gồm các xored là kết quả của phép XOR ở trên

Với mỗi từ thứ i có các khả năng:

- trong các xored[i] nếu tồn tại 1 xored[i] có giá trị hex nằm trong đoạn [20, 3F] hoặc lớn hơn hoặn bằng 7F thì vị trí của i chắc chắn không phải

dấu cách vì các ciphertext chỉ luôn chứa các kí tự thường

- sau khi loại trừ trường hợp trên thì khả năng ciphertext[i] là 1 dấu cách ' \s' phụ thuộc vào giới hạn b < n với số lượng giá trị hex của mỗi xored[i] nói trên nằm trong đoạn [01, 1F] là b.

  Với tập mã này thì em nhận thấy với n = 2 thì sẽ cho ra mã kết quả đẹp nhất có thể dự đoạn được nội dung

Sau khi duyệt hết các từ thứ i thì thu được 1 chuỗi là dạng khung của chuỗi cần tìm với kí hiệu '__' là kí tự chưa xác định chắc chắn không phải dấu cách. Còn lại '\s' là kí tự có xác suất cao là dấu cách (nhưng vẫn có thể là dấu khác)

Minh hoạ nằm trong 12 dòng đầu file 'result.txt' là kết quả khi sử dụng mã cần giải mã (mã số 11) XOR với tất cả các mã còn lại

Bước 2:

Xác định dạng khung của tất cả các chuỗi kí tự khác (kết quả nằm trong file 'over_view.txt')

Bước 3: Giải mã

Với kí tự thứ i của mã cần giải, xem xét xem kí tự thứ i của tất các các ciphertext còn lại có cái nào có khả năng là dấu cách không, nếu có XOR kí tự này với kí tự thứ i của mã cần giải ta thu được 1 khả năng của kí tự thứ i của mã cần giải. Xét trên tất cả các kí tự thứ i của các ciphertext còn lại ta được bộ các khả năng của kí tự thứ i của mã cần giải cho nó vào kết quả.

Xét trên tất các các kí tự của mã cần giảir và in kết quả ra file result.txt.

Bước 4: Dự đoán kết quả và kết luận

Sau khi có được kết quả từ bước 3. Dự đoán được mã cần giải là

'The secret message is: When using a string cipher, never use the key more than once'

Các kí tự dấu ':' và dấu ',' được dự đoán bởi kết quả từ bước 2 khi mà ở vị trí của dấu ':', ciphertext thứ 5 sau khi XOR với vị trí này của mã cần giải được hex là '1A' - là kết quả của việc XOR dấu ':' và dấu cách, tương tự cho dấu ','