2020 암호분석경진대회

1번 문제 : 고전 암호

힐 암호(Hill Cipher)는 $d \times d$의 행렬을 이용하여 d 블록 단위로 암호화하는 고전 암호이다. 암호화 키의 행렬을 $K = \begin{bmatrix} k_{11} k_{12} \cdots k_{1d} \\ k_{21} k_{22} \cdots k_{2d} \\ \vdots \ \vdots \ \ddots \\ k_{d1} k_{d2} \cdots k_{dd} \end{bmatrix}$라고 하자. 그러면 d개의 평문 $P = [p_1\, p_2\, \cdots\, p_d]$는 다음과 같이 암호화된다.

$$C = [c_1\, c_2\, \cdots\, c_d] = [p_1\, p_2\, \cdots\, p_d] \begin{bmatrix} k_{11} k_{12} \cdots k_{1d} \\ k_{21} k_{22} \cdots k_{2d} \\ \vdots \ \vdots \ \ddots \\ k_{d1} k_{d2} \cdots k_{dd} \end{bmatrix} \quad (c_i = p_1 k_{1i} + p_2 k_{2i} + \cdots + p_d k_{di})$$

또한 평문은 K의 역행렬을 이용하여 암호문은 다음과 같이 복호화된다.

$$P = [p_1\, p_2\, \cdots\, p_d] = [c_1\, c_2\, \cdots\, c_d] \begin{bmatrix} k_{11} k_{12} \cdots k_{1d} \\ k_{21} k_{22} \cdots k_{2d} \\ \vdots \ \vdots \ \ddots \\ k_{d1} k_{d2} \cdots k_{dd} \end{bmatrix}^{-1}$$

평문은 영문 소문자로만 구성되어 있고 이에 대응되는 암호문은 영문 대문자로만 구성되어있다고 가정하자.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
평문	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
암호문	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

그러면 각 암호문 c_i의 값은 26으로 나눈 나머지로 계산된다. $(c_i = p_1 k_{1i} + p_2 k_{2i} + \cdots + p_d k_{di} \pmod{26})$.

이러한 힐 암호는 (평문, 암호문) 쌍이 d개 이상이 주어진다면 쉽게 해독이 가능함이 알려져 있다. 즉, 알려진 평문 공격(Known Plaintext Attack)에서는 쉽게 해독이 가능하다. 하지만 암호문만 주어진 경우 해독이 쉽게 되지는 않는다. 다음과 같이 힐 암호의 암호문만 주어진 경우 평문 및 복호화 키 행렬을 찾고 분석 방법을 제시하시오.

HRDKHUBHAAMAEQMTMZSHGBAKFUBHAASYRXUNKYUAATQCTLUTOGEWVAJGVEIIYTKIOTQRXXQVSQL
ISVVOCNGCUXPKPIUBOHTVKCFKWNJSEZYSSUTUOESIXKAPVFXNZHAOQTLCGYJVAEHLNNKEESQMKSH
KKDFCNZSRHRDKHSDKFXVPTGMKRUPZBIKEVNYEKXMFXKFYMWYUDZDENEWNKDAOUXGPCXZDLCSNF
GCMCSNUAOJDBLQTAHEWYZCHQJYKSNUWOKQKONZGOKDXGUXKEMWQMCFGUEAVKHDIIATCHVTGYM
GKJMLNPCNAYKMIRWEETIYQKELEGLQOVKISFNUDAJQIQYBXQTMZSHGBAKFZRCNWRSODAFKKXWGAZG
DBIUDDHCUDFRFOVSZXADSHYSGLTQBMNEMKDCFSOZSRDYLIHIAXCMGMFEIDNZKOVJEOIEFNWWQEDR
LZYZIZXADSHYSGLJYFWDUAKSIOGOZOXWYPBUFEPNBIRJUJNDZJJYMURKNCIKPWLRMRIAGVSXTYNIWPR
OHLDHQOMBEKZURQCLQOVKISFNUAFQBHGPCLHZTPJVPXIZKLQSNVKIJAEITTNVSVWNFYVATDEMKDCT
GIHKZTVGZYXTYQEDBACFMNCAHRDKHSDKFXZXXGMJOSLPSZBMOILMMWRALAFFMNXXDYFBIYQVVOH
SWKGBIRJGTBYQLKIJAEQBTAXGFGAVUIJADHQKLFWRJXYFVIGGQZNBHSUIYOZALSKIABLWQNXNXKOAJAI
KHXODXWORVDOGBMHOPLQJZALQJZALIKTKLENZHQAVYUEUFEVLUXHGOWNMGWXUIAHGQOMNCKFQLI
PBNKVWDLNGMJCOBFKIGBYWPAHMMPQLUTOGECXITZVVAJEOIDCNWMFNLOBGQXCYFWQFWVXWRKWY
GBFHJVLBAWBOUQEKHZHSZZIZARYITDCLQFPGBTJMQVSQLIHPEJONCYMZWTVJVZOBOMOHPSXMPUKVA
GXIPOQUQUQBCKXZJSZAHEWYHAEMKOJCCCFBEUKVNCAWANSNXISVVOWHQGQFBGWKQEGBIFRGIZUJQ
WIMFANTGBHWGVAGXIPOQUQTTRMWDHDGRFENKYPZVCLNQAUBTZSRYGVGOWSVROENABMZTOHZRQ
FUEVPLLIODEYRYLUTOGPYAFHJFIVOSFMPBSHLEKWYWJYTFYETAZQCRFTFHOMACOQVTWKLKYMGIMQ
DSYNWMFNIEITWMBVVWANBQFVUSKZOTLCCWABAGHWZBZHRDKHDTUOMUUUGQICHNUUQFJYUCQUO