

# Information Security 2020

## 1<sup>st</sup> Project

**Prof. Junbeom Hur**

**TA. Dohyun Ryu**

Information System Security Lab.,  
Department of Computer Science and Engineering,  
Korea University, Seoul, Korea

# Hill Cipher

- Consider the hill cipher that uses  $d \times d$  key matrix to encrypt  $d$  characters
- In the hill cipher, encryption and decryption proceed as follows

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

- Each letter is assigned a number as follows

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
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	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

- Given the following 1285-byte ciphertext, find the corresponding plaintext

HRDKHUBHAAMAEQMTMZSHGBAKFUBHAASYRXUNKYUAATQCTLUTOGEWVAJGVEIYTKIOTQRXXQVSQ  
ISVOCNGCUXPKPIUBOHTVKCFKWNJSEZYSSUTUOESIXKAPVFXNZHAOQTLCGYJVAEHLNNKEESQMKSH  
KKDFCNZSRHRDKHSDKFVPTGMKRUPZBIKEVNYEKXMFXXFYMWYUDZDENENKDAOUXGPCXZDLCSNF  
GCMCSNUAOJDBLQTAHEWYZCHQJYKSNUWOKQKONZGOKDXGUXKEMWQMCFGUEAVKHDIATCHVTGYM  
GKJMLNPCNAYKMIRWEETIYQKELEGLQOVKISFNUDAJQIQYBXQTMZSHGBAKFZRCNWRSDAFKKXWGAZG  
DBIUDDHCUDFRFOVSZXADSHYSGLTQBMNEMKDCFSOZSRDYLIHAXCMGMFEIDNZKOVJEOIEFNWWQEDR  
LZYIZXADSHYSGLJYFWDUAKSIOGOZOXWYPBUEPNBIRJUJNDZJJYMURKNCIKPWLRMRIAGVSXTYNIWPR  
OHLDHQOMBKZURQCLQOVKISFNUAFQBHGPCCLHZZTPJVPXIZKLQSNVKIJAEITTNVSVWNFYVATDEMKDCT  
GIHKZTVGZYXTYQEDBACFMNCAHRDKHSDKFXXGJMOSLPSZBMOILMMWRALAFFMNXXDYFBIYQVVOH  
SWKGBIRJGTBYQLKIJAEQBTAXGFGAVUIJADHQKLFWRJXYFVIGGQZNBHSUIYOZALSKIABLWQNXNXKOAIAI  
KHXODXWORVDOGBMHOPLOJZALQJZALIKTKLENZHQAVYUEUFEVLUXHGOWNMGWXUIAHGQOMNCKFQLI  
PBNKVWDLNGMJCOBFKIGBYWPAHMMPLUTOGECCITZVVAJEOIDCNWMFNLOBGQXCYFWQFWVXWRKWY  
GBFHJVLBAWBOUQEKHZHSZZIZARYITDCLQFPGBTJMQVSQLIHPEJONCYMZWTJVJZOBOMOHPSXMPUKVA  
GXIPOQUQUQBCKXZJSZAHWEYHAEMKOJCCCFBEUKVNCAWANSNXISVVOWHQGFQBGWKQEGBIFRGIZUJQ  
WIMFANTGBHWGVAGXIPOQUQTTRMWDHDGRFENKYPZVCLNQAUBTZSRYGVGOWSVROENABMZTOHZRQ  
FUEVPLLIODEYRYLUTOGPYAFHJFIVOSFMPBSHLEKWWYJYTFYETAZQCRFTFHOMACQVTVWKLKYMIMQ  
DSYNWMFNIEITWMBVWWANBQFVUSKZOTLCCWABAGHWZBZHRDKHDTUOMUUUGQICHNUUQFJYUCQUO

# Hill Cipher

- Hint: You may utilize the following monogram and bigram frequency information
- Monogram frequencies

letter	a	b	c	d	e	f	g	h	i	j	k	l	m
%	8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	0.4	2.4
letter	n	o	p	q	r	s	t	U	V	w	x	Y	z
%	6.7	1.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.4	0.2	2.0	0.1

- Bigram frequencies

letter	TH	HE	IN	ER	AN	RE	ON	AT	EN	ND	TI	ES
%	3.55	3.08	2.43	2.05	1.99	1.85	1.76	1.49	1.45	1.35	1.34	1.34
letter	OR	TE	OF	ED	IS	IT	AL	AR	ST	NT	TO	
%	1.28	1.21	1.18	1.17	1.13	1.12	1.09	1.08	1.05	1.04	1.04	

1. Source code and exe file for solution **(25 points)**
2. Decrypted plaintext **(5 points)**
3. Report **(20 points)**
  - You need to show your solutions step by step
  - Appendix: Source code with comments

# Submission Guideline

- **Please upload the followings on Blackboard**

1. Source code and exe file for solution (**C is encourage, but if you want you can use Python, Java...etc**)
  2. Decrypted plaintext (**.txt, or image file**)
  3. Report (**.doc, .hwp, or pdf file**)
- Compress all of the files (**.zip**)

**– Late submission and any kind of plagiarism will result in 0 point**

## ASSIGNMENT SUBMISSION

Text Submission

Write Submission

Attach Files

Browse My Computer

Browse Content Collection

Browse Cloud Storage

Browse Dropbox

Attached files

File Name

Link Title

classical\_crypto\_2020xxxxxx.zip

classical\_crypto\_2020xxxx

Do not attach

# Submission Guideline

- **Deadline: 2020 Oct. 10, 23:59:00**
- **Late submission is not acceptable**