Information Security 2022
1st Project

Prof. Junbeom Hur

TA. Woonghee Lee

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

1st Project

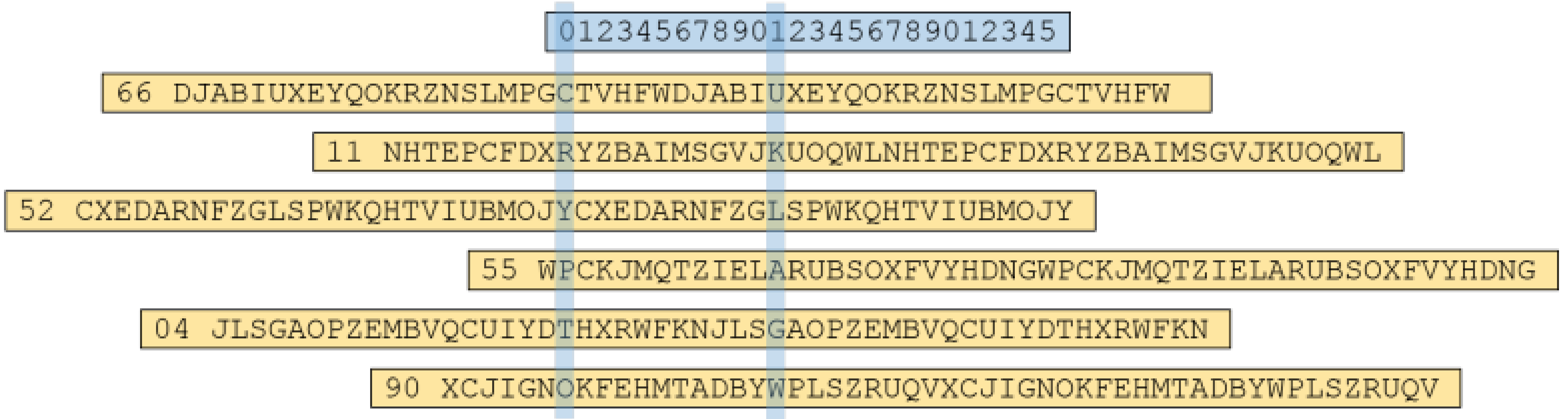
- We have a variant of the Vigenere cipher system using numbered strings as a key.
  - The strings used are given in the additional file.(100 strings)

- On each numbered string, the 26 capital letters of the alphabet are printed twice in a random order.

- A key pair looks like (66, 11, 52, 55, 04, 90 / 11), consisting of string numbers used followed by the offset between the plaintext column and the ciphertext column.
  - In the above key pair, 66, 11, 52, 55, 04, 90 are the key string numbers; 11 is the offset

1st Project

- Encryption Example
  - Plaintext: CRYPTO
  - Key = (66, 11, 52, 55, 04, 90 / 11)
- Put each string in a row so that ′CRYPTO′ comes out vertically according to the order of the key.
  - For each string, use a left (first) letter to make ′CRYPTO′
- As much as offset, each letter is shifted to the right, which become ciphertext.
- In this case, 'CRYPTO’ is encrypted to 'UKLAGW’.



```
                           01234567890123456789012345
    66 DJABIUXEYQOKRZNSLMPGCTVHFWDJABIUXEYQOKRZNSLMPGCTVHFW
               11 NHTEPCFDXRYZBAIMSGVJKUOQWLNHTEPCFDXRYZBAIMSGVJKUOQWL
52 CXEDARNFZGLSPWKQHTVIUBMOJYCXEDARNFZGLSPWKQHTVIUBMOJY
                       55 WPCKJMQTZIELARUBSOXFVYHDNGWPCKJMQTZIELARUBSOXFVYHDNG
       04 JLSGAOPZEMBVQCUIYDTHXRWFKNJLSGAOPZEMBVQCUIYDTHXRWFKN
                  90 XCJIGNOKFEHMTADBYWPLSZRUQVXCJIGNOKFEHMTADBYWPLSZRUQV
```

1st Project

- Offset can be an integer number from 1 to 25
- The number of strings used for a key do not exceed 25
    - $(N_{1,} N_{2,} N_{3, \ldots ,} N_{25} / O)$ is the form of a key
    - N_i is number of strings, and O is the offset
- No strings can be used twice in the key
    - E.g., (12, 25, 12, ..., / 24) is not allowed
- If the plaintext is longer than 25 letters, it divided into blocks of 25 letters
- All blocks are encrypted in the same way as the first block with the same key and offset

1st Project

- Problem:

- First 41 letters of plaintext:
  THISCIPHERWASWIDELYUSEDBECAUSEOFSIMPLESTR

- Ciphertext (125 letters):
  OYKWUXRNJOOPPTXCTYNYQHFCQNIIWNKPAZQSTIF
  HOOWEYEHDQQYZMFQDHGZWUQIEZOUJNCEHDQQE
  RBNJKRMRGLWIXVLVPFOBLLAVOPZENPADJPKVMMM
  PDYXJCBWEX

- Given the above ciphertext, find the plaintext of 125 letters and key

1st Project

- You should show the approachs step by step to decrypt the ciphertext.
- Hint: You may utilize the following mono, bi, tri, quadgram frequencies (n-gram frequencies)

- 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	4.0	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

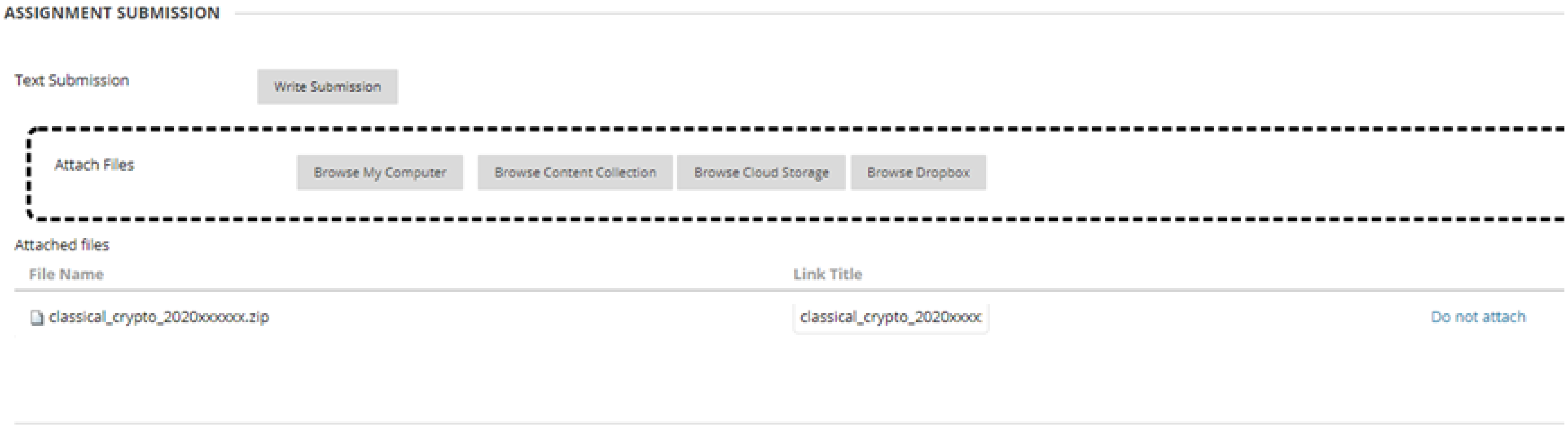
letter	TH	HE	IN	ER	AN	RE	ON	AT	EN	ND	TI	ES
%	3.55	3.08	2.43	2.05	1.99	1.85	1.76	1.49	1.45	1.35	1.34	1.34
letter	OR	TE	OF	ED	IS	IT	AL	AR	ST	NT	TO	
%	1.28	1.21	1.18	1.17	1.13	1.12	1.09	1.08	1.05	1.04	1.04	

Submission Guideline

- **Please upload the followings as a single compressed file into Blackboard**

1. Source codes and exe files for solution **(C is encouraged, but if you want you can use Python, Java, etc)**
2. Decrypted plaintext **(.txt, or image file)**
3. Report **(.doc, .hwp, or pdf file)**

❖ **Late submission, or any kind of plagiarism will result in 0 point**



ASSIGNMENT SUBMISSION

Text Submission

Attach Files

Attached files

File Name	Link Title	
classical_crypto_2020xxxxxx.zip	classical_crypto_2020xxxx	Do not attach

Submission Guideline

- Deadline: 2022. Oct. 27, 23:59
- Late submission is not acceptable