

# Approved Extension Request, Now Due: 30/08/2022 11:59pm AEST

We've processed your Assignment extension request FORM-AEX-178701



no-reply@qut.edu.au  
To Ash Phillips



Fri 26/08/2022 1:53 PM

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Hi Ashley,

Thank you for your assignment extension request.

We have **approved your request (FORM-AEX-178701)**. The due date for your assignment **Assignment 1 - historical cryptanalysis & info theory**, for unit CAB340 has been extended **until 30/08/2022 11.59pm AEST**.

Please note, this is the maximum extension available for this assessment item. If you feel that the work you submit on this due date has been impacted, you may wish to apply for Special Consideration. If you have any questions regarding the length of extension, please contact your Unit Coordinator in the first instance.

You are responsible for ensuring that this assignment is eligible for extension before submitting it after the original due date. Check your [unit outline](#) for eligibility.

Be aware that a copy of this email is kept on file. You should not alter this email in any way. Email notifications that have been altered or differ in any way from the original may result in an allegation of student misconduct as set out in the [Student Code of Conduct](#).

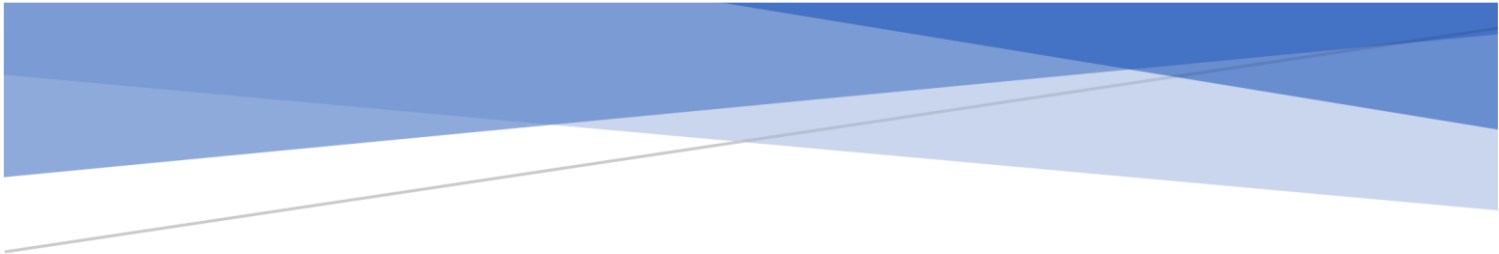
**Need extra support?** You can access free, confidential [counselling with qualified professionals](#). We also offer [planning and support if you have a disability, injury or health condition](#) that affects your ability to study. If you are struggling to meet your university commitments, [academic support](#) is also available.

**Have a question?** You can contact us by email or phone. We're also available to help you on campus or via online chat. Visit the [HiQ website](#) for our contact details and opening hours.



You have received this email because you have submitted an assignment extension request. View our [Privacy and Security statement](#).

Ref ID: 10477659 FORM-AEX-178701



# ASSESSMENT 1: CRYPTANALYSIS OF HISTORICAL CIPHERS, INFORMATION THEORY FOR CRYPTOGRAPHY

CAB340: Cryptography

Ash Phillips, n10477659

Used Folder: 059

Extended Due Date: 30/08/22, 11:59 pm

## 1.0. Cryptanalysis of Historical Ciphers

### 1.1. Cryptanalysis Tasks

Folder Used - 059

(a)

#### **Simple Random Substitution Cipher:**

The statistics needed include the frequency distribution of the ciphertext characters for comparison with the typical distribution in English text as well as any patterns, digrams/trigrams, or typical word shapes/spacings.

To recognise this cipher the index of coincidence can be calculated to compare the character frequencies to a normal distribution – if the value is close to 0.06 it is likely to be a substitution cipher – then through cryptanalysis, assuming English plaintext, the most common characters could be hypothesised as E and/or T (the most used letters in English).

#### **Vigenère Cipher:**

The statistics needed include any repetitions present in the ciphertext and the length(s) between them (separations of  $d$  threads).

These statistics could be used to both recognise and cryptanalyze the cipher as the encryption key repeats itself every  $d$  letters, meaning if repetition occurs in the plaintext in alignment with these repetitions of the key, these same repetitions will also be present in the ciphertext offset in multiples of  $d$  letters (which is a characteristic of Vigenère cipher), giving the opportunity to hypothesize the key size  $d$ .

#### **Simple Transposition Cipher:**

The statistics needed are the frequency distributions of the ciphertext characters.

These statistics could be used to recognise the cipher as the character frequency distribution of the transposition cipher is the same as the plaintext and therefore similar to English, then, once recognised the process of anagramming the cipher text can be performed to cryptanalyze it.

#### **2x2 Hill Cipher:**

The statistics needed to be collected are the frequency distribution of the polygrams of the ciphertext characters (groups of 2 characters instead of individual).

These statistics could be used to recognise the cipher by comparing these grouping frequencies to the frequency of regular English to see if similar patterns emerge, then, through cryptanalysis, assumptions can be made as to the possible plaintext mappings and a known-plaintext attack can be attempted.

## Assessment 1: Cryptanalysis of Historical Ciphers, Information Theory for Cryptography

(b)

### File A:

Cipher Used	Simple Transposition Cipher
Encryption Key	EDABFHICGNMJKOQRLP
First Hundred Letters of Recovered Plaintext	h spirits at that moment so far from sorrow sadness or selfreproach that she purposely deceived herself as young people often do No I am too happy now to spoil my enjoyment by sympathy with anyones sorrow she felt and she said to herself No I must be mistaken he must be feeling happy just as I am

### File B:

Cipher Used	Vigenère Cipher
Encryption Key	CDNGCDWEK
First Hundred Letters of Recovered Plaintext	w to be the enemys troops The weather had cleared again since noon and the sun was descending brightly upon the Danube and the dark hills around it It was calm and at intervals the bugle calls and the shouts of

### File D:

Cipher Used	Simple Random Substitution Cipher
Encryption Key	kztvwbjfqmxrpgchcdliysnoea
First Hundred Letters of Recovered Plaintext	f as if to blow his nose and seeing the knot in it pondered shaking his head sadly and significantly And I have a great favor to ask of you Papa said he Hm said the count and stopped I was driving past Yuspovs house just now said Berg with a laugh when the steward a man I know ran out and asked me whether I wouldnt buy something I went in out of

(c) Extra Credit

### File C:

Cipher Used	2x2 Hill Cipher
Encryption Key	$\begin{bmatrix} 11 & 20 \\ 0 & 25 \end{bmatrix}$
First Hundred Letters of Recovered Plaintext	be responsible for what might happen On the evening of the day the old prince died the Marshal went away promising to return next day for the funeral But this he was unable to do for he received tidings that the French had unexpectedly advanced and had barely time to remove his own family and valuables from his estate For some thirty years Boguchrovo had been managed by the village Elder Dron whom the old prince called by the diminutive Drnushka Dron was one of those physically and mentally vigorous peasants who grow

	big beards as soon as they are of age and go on unchanged till they are sixty or seventy without a gray hair or the loss of a too
--	-----------------------------------------------------------------------------------------------------------------------------------

## 2.0. Information Theory in Cryptography

### 2.1. Perfect Secrecy of Constrained Historical Ciphers

(a)

Yes, perfect secrecy is achieved as all 26 keys available to the cipher are used in equal probability so no information can be gained through cryptanalysis.

(b)

Yes, perfect secrecy is achieved as with 1 letter only no information can be gained through cryptanalysis; nothing is shown via character frequency distributions.

(c)

No, perfect secrecy is not achieved as the key is smaller than the length of the message and information can be gained through analysis of character frequencies.

(d)

No, perfect secrecy is not achieved as once again information can be gained through statistical analysis on the distribution of character frequencies.

(e)

No, perfect secrecy is not achieved as, while an equal size for block length  $d$  and plaintext meets the first condition of the onetime pad, once again information can be gained through frequency distributions.

(f)

No, perfect secrecy is not achieved as, though no information could be gained through character frequencies, the positions of characters and word lengths common in English can provide information.

(g)

Yes, perfect secrecy is achieved as the first condition of the onetime pad is met (as  $l=d$ ) and, although character frequencies can be analysed from the ciphertext, this information is already known meaning no extra information was gained, therefore passing the conditions of perfect secrecy.

## 2.2. Entropy and Conditional Entropy

**Values Used:**  $q = 0.01$ ,  $n = 10477659$ ,  $r = 2019$

(a)

**Symbolic Expression:**

$$H(V) = \left( \frac{qn + r(1 - q)}{n} \right) \log_2 \left( \frac{rn}{qn + r(1 - q)} \right) + (n - r) \left( \frac{1 - q}{n} \right) \log_2 \left( \frac{n}{1 - q} \right)$$

**Numeric Evaluation:**

$$H(V) = \left( \frac{106775.4}{10477659} \right) \log_2 \left( \frac{21154393521}{106775.4} \right) + \left( \frac{10370883.6}{10477659} \right) \log_2 \left( \frac{10477659}{0.99} \right)$$

$$H(V) = \mathbf{23.2768 \text{ bits}}$$

(b)

**Symbolic Expression:**

$$H(F|V) = \left( \left( \frac{qn + r(1 - q)}{n} \right) \log_2 \left( \frac{rn}{qn + r(1 - q)} \right) + (n - r) \left( \frac{1 - q}{n} \right) \log_2 \left( \frac{n}{1 - q} \right) \right) - \left( q \log_2 \left( \frac{1}{q} \right) + (1 - q) \log_2 \left( \frac{1}{1 - q} \right) \right)$$

**Numeric Evaluation:**

$$H(F|V) = \mathbf{23.2960 \text{ bits}}$$

(c)

As HRNG is a random number generator with a large  $n$  value the expected entropy was high, as was evaluated. From the evaluations entropy (a) was calculated to be slightly less than conditional entropy (b); with a difference of 0.0192. This is likely because  $n$  was much larger than  $r$ . Due to this  $r$  made little difference on entropy, as showcased in the evaluation of the conditional entropy as the condition of the fault showed only a slight difference.

(d)

Yes. As it was seen with the current  $n$  value, the fault made little difference to the entropy of the HRNG meaning it is highly likely that if  $n$  were to be increased this affect would minimise even further, overcoming the bugginess.