# COSC2539: Security in Computing and IT

# Assignment 1

# Part 2 Cryptography Semester B, 2017

REPORT

Lecturer: Denis Rinfret

Students:

Minh Tran Van - s3585377

Tuan Le Nguyen Anh - s3574983

### Assignment Objective

The aim of this assignment is to comprehend the abstraction of cryptography by using programing language to write algorithms in order to decrypt several cipher-texts base on provided keys or encrypting algorithms.

### Technique

Java has been used to write decoding algorithm, due to its object-oriented characteristic.

### Strategy for Decryption

Caesar

For this encrypting algorithm, in unknown-key case, each character in the cipher text has been taken to be transformed into equivalent characters in 49 shifted alphabets, then these 49 results will be processed by scoring algorithm to sort out top of three results based on looking up the English dictionary. (/src/decryption/Caesar.java)

Columnar Transposition

Firstly, the algorithm for calculating common divisors is called. After having the common divisors, another algorithm processes the cipher text message to construct the plain text messages. Similar to Caesar, the scoring algorithm will find out the top three results. (/src/decryption/Transposition.java)

Caesar & Columnar Transposition

The algorithm for this case is a collaboration of previous decryption methods. After having the results from columnar transposition’s decoding algorithm, these results will be continually decrypt by caesar's code. (/src/decryption/ComboEncryption.java)

Random Substitution

The strategy for decrypting random substitution is far more complicated than the previous ones. Consequently, algorithm that automatically decrypts the message has not been developed and the process must be assisted by human.

Firstly, the Monogram Analysis method counts the frequencies of all characters in the cipher-text and creates a Frequency Table file. The Space Analysis algorithm then transforms each character into white space to test out which character is most likely to be the space character. In this case, the one which generates the lowest longest-word has the higest likelihood to be the space character. The Get One Letter Word From Cipher method is then called to return one-letter words from the cipher text. The one with highest frequency is assumed to be the “A” character “A” and “I” are the most common one-letter words in English and “A” is more common than “I” in academic writing. Next, other two-letter words in which one letter is known are guessed using a two-letter-word dictionary. The process is repeated until the key is fully identified. (/src/decryption/RandomSubstitution.java)

Vernam

Different chunks of letters with length equal to the length of cipher-text are used as key for the Vernam cipher. The results are then scored and sorted to print out top three results. (/src/decryption/Vernam.java)

### Results

Question 1:

Key: 39

Plain text:

LIVING IN VIETNAM

LOCATED IN SOUTH EAST ASIA, VIETNAM OCCUPIES THE SOUTH OF THE INDOCHINA PENINSULA WITH THE SHAPE OF AN ELONGATED 'S'. A TROPICAL COUNTRY, VIETNAM HAS DIVERSE SCENERY: FROM SOARING MOUNTAINS TO WHITE SANDY BEACHES, FROM TROPICAL FORESTS TO MYSTERIOUS CAVES.

VIETNAM IS ALSO WHERE YOU CAN FIND A FEAST OF HISTORY AND CULTURE. VIETNAMESE CULTURE IS DISTINCT: A FUSION OF CHINESE, JAPANESE, AMERICAN AND FRENCH CULTURES.

THE COUNTRY IS DIVIDED INTO THREE AREAS: NORTH VIETNAM, CENTRAL VIETNAM AND SOUTH VIETNAM. WHILE THE NORTH IS KNOWN FOR ITS OLD AND HISTORIC CAPITAL, CENTRAL VIETNAM IS FAMOUS FOR ITS SPECTACULAR BEACHES AND LAGOONS. COMING TO THE SOUTH, YOU WILL ENCOUNTER DYNAMIC HO CHI MINH CITY'S MODERN LIFE. LIVING AND STUDYING IN VIETNAM WILL YOU AN OPPORTUNITY TO EXPLORE A UNIQUE, HISTORIC, EXOTIC, YET RAPIDLY DEVELOPING COUNTRY.

Question 2:

Key: 18

Plain text:

HEALTH CARE SERVICES AND SAFETY CONCERN

MOVING AWAY FROM HOME, THE ALTERATIONS IN CLIMATE, IN LIVING ENVIRONMENT ARE SIGNIFICANT FACTORS AFFECTING ONE'S HEALTH CONDITION. IT IS IMPORTANT FOR INTERNATIONAL STUDENTS TO TAKE CARE OF THEIR HEALTH. IT IS RECOMMENDED THAT BEFORE TRAVELLING TO VIETNAM, YOU SHOULD PURCHASE PRIVATE HEALTH INSURANCE TO HELP COVER THE COST OF TREATMENT AT PRIVATE HEALTHCARE ESTABLISHMENTS.

AMONG THE WIDE RANGE OF HOSPITALS AND DIFFERENT STANDARDS OF HEALTHCARE, PRIVATE HOSPITALS ARE GENERALLY ON PAR WITH THOSE IN THE WESTERN COUNTRIES AND ACCEPT INTERNATIONAL HEALTH INSURANCE. THE MAJORITY OF DOCTORS ARE FROM THE US, KOREA, JAPAN AND FRANCE, AS WELL AS OVERSEAS-TRAINED VIETNAMESE DOCTORS.

AT RMIT VIETNAM, THE HEALTH AND SAFETY OF THE STUDENTS IS A TOP PRIORITY. WE HAVE 24-HOUR SECURITY, HEALTH CENTRES AND COUNSELLING SERVICES ON CAMPUS.

Question 3:

Algorithm:

Columnar Transposition

Key: 20

Plain text:

'RMIT UNIVERSITY VIETNAM PROVIDES PROGRAM SPECIFIC INTERNSHIPS. DURING THE INTERNSHIP STUDENTS ARE ENROLLED INTO SPECIFIC INDUSTRY-BASED COURSES THAT INTEGRATE THE STUDENT'S THEORETICAL KNOWLEDGE WITH WORKPLACE EXPERIENCE. STUDENTS TAKE ON A RANGE OF FINITE PROJECTS THAT EMPLOYERS CAN HELP IDENTIFY, WHILE RMIT UNIVERSITY VIETNAM PROVIDES CLOSE ACADEMIC SUPERVISION. THIS GIVES A RICHER EDUCATIONAL EXPERIENCE AND IMPORTANT SKILLS MAKING STUDENTS MORE WORK-READY UPON GRADUATION.

THE INTERNSHIPS HAVE PROVEN BENEFICIAL FOR A PLETHORA OF COMPANIES WHO HAVE BEEN ABLE TO "TRIAL RUN" RMIT UNIVERSITY VIETNAM STUDENTS FOR POSSIBLE OFFICIAL EMPLOYMENT LATER. ‘

Question 4:

Key: ‘D’ -> ‘ ‘ (white space), ‘L’ -> ‘E’, ‘P’ -> ‘O’, ’N’ -> ’N’, ‘1’ -> ’T’, ‘K’ -> ‘I’, ‘(‘ -> ‘A’, ‘.’ -> ‘R’, ‘:’ -> ’S’, ‘J’ -> ‘L’, ‘,’ -> ‘U’, ‘8’ - > ‘Y’, ‘R’ -> ‘G’, ‘I’ -> ‘D’, ‘Y’ -> ‘H’, ’T’ -> ‘P’, ‘O’ -> ‘M’, ‘ ‘ (white space) -> ‘C’, ‘?’ -> ‘F’, ’\n’ -> ‘V’, ‘3’ -> ‘W’, ‘X’ -> ‘.’, ‘Q’ -> ‘B’, ‘2’ -> ‘,’, ‘G’ -> ‘K’, ‘-‘ -> ’\n’, ‘$’ -> ‘’’ (single quote), ’S’ > ‘-‘, ‘M’ -> ‘X’, ‘!’ -> ‘J’.

Plan text:

RMIT VIETNAM IS A GLOBAL UNIVERSITY OF TECHNOLOGY AND DESIGN...

TECHNOLOGY NOW UNDERPINS SO MANY ASPECTS OF MODERN LIFE. WHETHER YOU ARE READING THE NEWS FROM YOUR LAPTOP, BUYING MOVIE TICKETS ON YOUR SMARTPHONE ON THE WAY TO THE CINEMA, OR USING A RECIPE APP ON YOUR TABLET WHILE YOU COOK - TECHNOLOGY HAS BECOME INTEGRATED WITH OUR DAILY EXISTENCE.

TAKING A DEGREE IN A AN IT-RELATED FIELD MEANS LEARNING SKILLS THAT HELP TO SOLVE PEOPLE'S PROBLEMS IN CREATIVE, INNOVATIVE WAYS, USING TECHNOLOGY TO TRANSFORM PEOPLE'S WORLDS. IF YOU'RE INTERESTED IN BEING A LEADER IN A CUTTING EDGE INDUSTRY, YOU MAY HAVE JUST FOUND YOUR FUTURE.

Question 5

Key: A GLOBAL UNIVERSITY OF TECHNOLOGY AND DESIGN...

TECHNOLOGY NOW UNDERPINS SO MANY ASPECTS OF MODERN LIFE. WHETHER YOU ARE READING THE NEWS FROM YOUR LAPTOP, BUYING MOVIE TICKETS ON YOUR SMARTPHONE ON THE WAY TO THE CINEMA, OR USING A RECIPE APP ON YOUR TABLET WHILE YOU COOK - TECHNOLOGY HAS BECOME I

Plain text:

WHAT IS INFORMATION TECHNOLOGY?

INFORMATION TECHNOLOGY IS ABOUT FINDING THE BEST SOLUTIONS TO MANAGE INFORMATION USING COMPUTERS AND SOFTWARE. IT PROFESSIONALS USE CUTTING EDGE TECHNOLOGIES TO STORE, PROTECT, PROCESS, TRANSFER AND RETRIEVE INFORMATION SO THAT ORGANISATIONS CAN RUN MORE EFFICIENTLY.

Question 6

Key: 40

Plain text:

THE BACHELOR OF INFORMATION TECHNOLOGY PROGRAM IS ACCREDITED AT THE PROFESSIONAL LEVEL BY THE AUSTRALIAN COMPUTER SOCIETY (ACS), AN ORGANISATION THAT ACCREDITS INFORMATION AND COMMUNICATION TECHNOLOGY RELATED PROGRAMS IN AUSTRALIA.QQQQQQQQQ

Question 7

Key: ‘F’ -> ’ ’ (white space), ’T’ -> ‘E’, ‘$’ -> ‘I’, ‘H’ -> ’T’, ‘J’ -> ‘A’, ‘2’ -> ’N’, ‘A’ -> ‘R’, ‘“‘ (double quote) -> ‘O’, ‘U’ -> ’S’, ‘0’ -> ‘L’, ‘Q’ -> ‘M’, ‘4’ -> ‘D’, ‘7’ -> ‘C’, ‘L’ -> ‘U’, ‘-‘ -> ‘G’, ‘1’ -> ‘V’, ‘K’ -> ‘H’, ‘Z’ -> ‘F’, ‘9’ -> ‘P’, ‘Y’ -> ‘Y’, ‘D’ -> ‘B’, ‘ ‘ (white space) -> ‘.’, ‘B’ -> ‘W’, ’S’ -> ‘,’, ’N’ -> ’\n’ , ‘P’ -> ‘Q’, ‘8’ > ‘-‘, ‘C’ -> ‘K’, ‘?’ -> ‘X’, ‘6’ -> ‘’’ (single quote)

Plan text:

TEACHING AND LEARNING AT RMIT VIETNAM

RMIT VIETNAM IS COMMITTED TO PROVIDING QUALITY EDUCATION. THE DEGREE YOU WILL RECEIVE AFTER SUCCESSFUL COMPLETION OF YOUR STUDIES IN VIETNAM IS A GLOBAL RMIT UNIVERSITY DEGREE. THE LEARNING OUTCOMES AND ASSESSMENTS FOR COURSES TAUGHT IN VIETNAM ARE EQUIVALENT TO THOSE DELIVERED AT RMIT MELBOURNE. ACADEMIC STAFF EMPLOYED AT RMIT INTERNATIONAL UNIVERSITY VIETNAM WORK IN COLLABORATION WITH ACADEMIC STAFF FROM RMIT UNIVERSITY MELBOURNE TO CUSTOMISE THE MATERIALS THAT ARE PREPARED IN MELBOURNE FOR DELIVERY IN VIETNAM, AND TO FACILITATE THE TEACHING AND LEARNING PROCESSES AT RMIT VIETNAM. THE ACADEMIC'S ROLE AT RMIT VIETNAM IS FOCUSED ON ADDING VALUE TO THE TEACHING AND LEARNING PROCESS THROUGH CREATIVE FACILITATED LEARNING. THE TEACHING AND LEARNING MODEL AT RMIT VIETNAM IS BASED ON INTERNATIONAL BEST PRACTICE AND INCLUDES CLASSROOM LEARNING EXPERIENCES, FACILITATED ON-LINE AND SELF-DIRECTED LEARNING BY STUDENTS, AND PEER LEARNING.