QUIZ GSLC COMP6547 – Network Cryptography

Pert5 – Encrypting and Decrypting Files

KD Dosen : D4587

KELAS : LA07

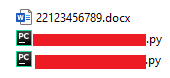
NIM :2201744935

NAMA : AlbertAdiwena.S

**JAWAB :**

**File yang diupload ke Assignment Binusmaya adalah [NIM].ZIP**

**Folder 2212345678 isinya file ini + file-file .py :**

****

**di ZIP menjadi 2212345678.zip**



1. **Code Python for Hacking Affine Cipher : function hackAffine (80%)**

**Lampirkan affineHacker.py Code Anda yang telah dilengkapi function hackAffine**

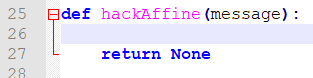
1. **Dokumentasikan function hackAffine yang anda buat tersebut (20%)**

**SOAL**

**Gunakan Text editor pilihan anda :**

* 1. **PyCharm :** <https://www.jetbrains.com/pycharm/>
  2. **vscode :** <https://code.visualstudio.com/docs/languages/python>
  3. Notepad++, Sublime, etc

1. **Code Python for Hacking Affine Cipher : function hackAffine (80%)**



**Dengan referensi Code yang ada di Slide #8 - #11, S, buatlah code untuk hackAffine yang terdiri dari :**

* + - * **Validasi key valid:**

**def checkKeys(keyA, keyB, mode):**

**if keyA == 1 and mode == 'encrypt':**

**sys.exit('Cipher is weak if key A is 1. Choose a different key.')**

**if keyB == 0 and mode == 'encrypt':**

**sys.exit('Cipher is weak if key B is 0. Choose a different key.')**

**if keyA < 0 or keyB < 0 or keyB > len(SYMBOLS) - 1:**

**sys.exit('Key A must be greater than 0 and Key B must be between 0 and %s.' % (len(SYMBOLS) - 1))**

**if cryptomath.gcd(keyA, len(SYMBOLS)) != 1:**

**sys.exit('Key A (%s) and the symbol set size (%s) are not relatively prime. Choose a different key.' % (keyA, len(SYMBOLS)))**

* + - * **Menggunakan function Decrypt Affine Cipher:**

**def decryptMessage(key, message):**

**keyA, keyB = getKeyParts(key)**

**checkKeys(keyA, keyB, 'decrypt')**

**plaintext = ''**

**modInverseOfKeyA = cryptomath.findModInverse(keyA, len(SYMBOLS))**

**for symbol in message:**

**if symbol in SYMBOLS:**

**# Decrypt the symbol:**

**symbolIndex = SYMBOLS.find(symbol)**

**plaintext += SYMBOLS[(symbolIndex - keyB) \* modInverseOfKeyA % len(SYMBOLS)]**

**else:**

**plaintext += symbol # Append the symbol without decrypting.**

**return plaintext**

* + - * **Mendeteksi apakah hasil decrypt merupakan bahasa inggris**

**def isEnglish(message, wordPercentage=20, letterPercentage=85):**

**# By default, 20% of the words must exist in the dictionary file, and**

**# 85% of all the characters in the message must be letters or spaces**

**# (not punctuation or numbers).**

**wordsMatch = getEnglishCount(message) \* 100 >= wordPercentage**

**numLetters = len(removeNonLetters(message))**

**messageLettersPercentage = float(numLetters) / len(message) \* 100**

**lettersMatch = messageLettersPercentage >= letterPercentage**

**return wordsMatch and lettersMatch**

1. **Dokumentasikan function hackAffine yang anda buat tersebut (20%)**

**Mengerjakan Assignment yang diupload di menu Assignment secara perorangan tanpa plagiarism.**

**- File yang diupload ke Assignment Binusmaya adalah [NIM].ZIP berisi 1 .docx + affineHacker.py**

**- Deadline : Kamis, 7 Mei 2020 23:59**