

DAT234

Powershell oppgave

07.09.2018

Universitet i Agder

Idris Amrandi, Aslak Granåsen og Sindre Pedersen Fosser.

Innledning

Med denne oppgaven ønsket vi lære hvordan man kan skrive en enkel algoritme som kan brukes til å dekryptere en melding/tekst (Lfzcpbse!opu!gpvoe!/Qsftt!G2!up!dpoujovf). Vi skulle også finne ut av hvordan vi kunne gjøre det motsatte, altså å kryptere en melding. Dette er noe vi føler er viktig fordi det å kunne kryptere og dekryptere enkle meldinger er en veldig god innledning til dette temaet, hvor man da kan senere bygge på denne kunnskapen for å kunne jobbe med mer avanserte algoritmer.

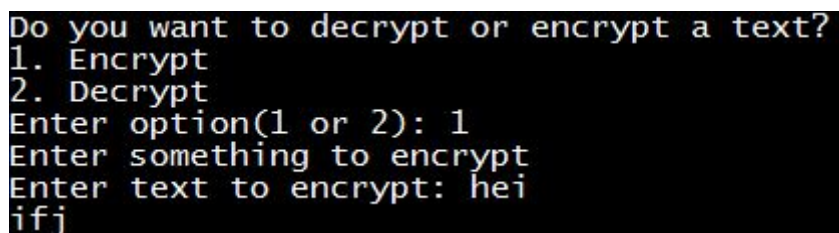
Installasjoner

Vi brukte Powershell ISE som allerede er installert på de siste Windows versjonene. For å kunne kjøre scripts som vi lagde måtte vi endre på dens execution policy med kommandoen “set-executionpolicy” samtidig som at man måtte kjøre Powershell som administrator for å kunne bruke kommandoen. Etter det var gjort, var vi klar for å begynne å lage scripts.

Arbeid utført

Vi har laget script som kan:

- Kryptere en melding



```
Do you want to decrypt or encrypt a text?  
1. Encrypt  
2. Decrypt  
Enter option(1 or 2): 1  
Enter something to encrypt  
Enter text to encrypt: hei  
ifj
```

- Dekryptere en melding

```
Do you want to decrypt or encrypt a text?
1. Encrypt
2. Decrypt
Enter option(1 or 2): 2
Enter text to decrypt: ifj
hei
```

- Kryptere ved bruk av base64 encoding med 2 som modifier i encrypt funksjonen

```
Do you want to decrypt or encrypt a text?
1. Encrypt
2. Decrypt
3. Encrypt(Secure)
4. Decrypt(Secure)
Enter option(1 or 2): 3
Enter string: : hei
awBoAGwA
```

- Dekryptere ved bruk av base64 encoding med 2 som modifier i decrypt funksjonen

```
Do you want to decrypt or encrypt a text?
1. Encrypt
2. Decrypt
3. Encrypt(Secure)
4. Decrypt(Secure)
Enter option(1 or 2): 4
Enter string: : awBoAGwA
kh1
hei
```

Når vi testet det vi hadde laget fungerte det, men vi oppdaget at det ikke ville kjøre på enkelte av våre PC'er pga. en syntaksfeil (som ikke dukket opp på enkelte maskiner). Løsningen var at flere steder i koden måtte vi legge til "{" "}" før og etter "global". Vi er ikke sikre på det er noen annen grunn til at det fungerer på noen maskiner, og ikke på andre.

Resultater

Ved bruk av den dekrypteringsmetoden som var i oppgaven, fant vi ut av at den krypterte meldingen (som var Lfzcpbse!opu!gpvoe!/Qsftt!G2!up!dpoujovf) var egentlig "Keyboard not found. Press F1 to continue". På bildet under kan man se resultatet.

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Bruker\Desktop\oiuopk>"C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe"
e p1-4.ps1
Do you want to decrypt or encrypt a text?
1. Encrypt
2. Decrypt
Enter option(1 or 2): 2
Enter text to decrypt: Lfzcpbse!opu!gpvoe/!Qsftt!G2!up!dpoujovf
:Keyboard not found. Press F1 to continue

C:\Users\Bruker\Desktop\oiuopk>pause
Press any key to continue . . .
```

Vi fikk til alle oppgavene, så det var ikke noe problemer som vi møtte på som førte til noen uløste oppgaver.

Konklusjoner/erfaringer

Oppgavene gikk omtrent som forventet, og vi ble møtt med få problemer (med et par unntak). Som et resultat har vi lært litt mer om krypteringsalgoritmer og scripting i praksis.