

TI-Nspire CX II

Achtergrondinformatie



Hedy Lamarr 1944

- Hedy Lamarr was een trendy Oostenrijks-Amerikaanse filmactrice en werd opgenomen in de National Inventor's Hall of Fame voor haar werk aan radiofrequentie-hoppende spreidingsspectrum radargestuurde torpedo's die werden gebruikt in de Tweede Wereldoorlog. Haar uitvinding ontving het [Amerikaanse patent 2.292.387](#). Deze methode om radioberichten te verbergen houdt in dat kleine delen van een bericht over verschillende radiofrequenties worden verzonden. De zender en ontvanger stemmen af op een lijst van kanalen die gebruikt zullen worden om het bericht te verzenden en te ontvangen. Wanneer het eerste bit van het bericht op het eerste kanaal in de lijst wordt verzonden, schakelen de zender en ontvanger hun radio's over naar het volgende kanaal op de lijst. Elk bit van het bericht wordt over een ander radiofrequentiekanaal verzonden totdat het gehele bericht is verstuurd. Zolang de lijst van kanalen geheim wordt gehouden voor een hacker, kan het bericht niet gemakkelijk worden onderschept. Deze activiteit genereert de kanaallijst op basis van een privésleutel die gedeeld wordt tussen de zender en ontvanger.

Wat is jouw opdracht?

1. Oefen op het maken van een lijst in Python waarin je de kanalen opslaat:
 - Elk groepslid moet naar de pagina met '**Oefenen_korte_sleutel.py**' gaan en het programma uitvoeren.
 - Ga vervolgens naar de pagina met het programma '**Oefenen_lange_sleutel.py**'.
 - Deze twee programma's maken elk een kanaallijst die afhankelijk is van de sleutel. Wat is het verschil tussen de uitkomsten van de twee programma's? Genereert een korte sleutel of een lange sleutel meer kanalen? Welke kanaallijst zou veiliger zijn?
2. Een bericht sturen met behulp van frequentiehopping spreidingsspectrum:
 - De ontvanger:
 - Ga naar '**student_ontvanger.py**', verander de groep naar je toegewezen nummer en voer het programma uit **voordat** de zender hun programma heeft uitgevoerd.
 - De zender:
 - Ga naar '**student_zender.py**', verander de berichtstring en de groep naar je toegewezen nummer, en voer het programma uit **nadat** de ontvanger en de hacker hun programma's hebben gestart.
 - De hacker:
 - Ga naar '**student_hacker.py**', verander de groep naar je toegewezen nummer en voer het programma uit **voordat** de zender hun programma heeft uitgevoerd.
 - Nadat je team de activiteit heeft uitgevoerd, moet de zender het **bericht** en de **sleutel** wijzigen en de sleutel alleen met de ontvanger delen. Vertel de hacker de nieuwe sleutel niet; **houd deze privé!** Kan de hacker je bericht in leesbare tekst lezen zoals ze deden in de 'All Clear' activiteit?

De code

Zender

```

student_zender.py 11/11
from microbit_radio import *
from frequency_hoppen import *
# De lijst van de kanalen en groep moeten
# hetzelfde zijn als de ontvanger.
groep = 1
sleutel = "Timbuktu"
kanaal_list = maak_list_van_kanalen(sleutel)
bericht = "Goud verstopt in koekjestrommel."
clear_history()
print("\nBericht =",bericht)
tx(bericht,list_van_kanalen,groep)
    
```

Ontvanger

```

*student_ontvanger.py 11/13
from microbit_radio import *
from frequency_hoppen import *
# Geheime sleutel en groep moeten hetzelfde zijn
# als de ontvanger. Het kanaal zal automatisch
# veranderen als het programma loopt.
groep = 1
sleutel = "Timbuktu"
kanaal_list = maak_list_van_kanalen(sleutel)
clear_history()
bericht = rx(list_van_kanalen,groep)
print("\nBericht =",bericht)
    
```

Hacker

```

*student_hacker.py 11/13
from microbit_radio import *
from frequency_hopping import *
# Geheime sleutel en groep moeten hetzelfde zijn
# als de ontvanger. Het kanaal zal automatisch
# veranderen als het programma loopt.
groep = 1
sleutel = "Zanzibar"
kanaal_list = maak_list_van_kanalen(sleutel)
clear_history()
bericht = rx(list_van_kanalen,groep)
print("\nBericht =",bericht)
    
```

Extra uitdagingen

- Voer de activiteit opnieuw uit in een andere teamrol.
- Herhaal de activiteit met verschillende sleutels en berichten.
- Probeer te ontdekken hoeveel kanalen er op de lijst staan voor een gegeven sleutel.

Samengevat

- Om te kunnen communiceren, moeten twee radio's op hetzelfde kanaal en dezelfde groep zitten.
- Een zendprogramma kan het kanaal wisselen na het verzenden van elk teken.
- Een ontvangend programma moet van tevoren weten welke kanalen de zender zal gebruiken om het bericht te versturen.
- Het gebruik van een frequentiehopping-algoritme, zoals het algoritme in deze activiteit, kan het hacken moeilijker maken.

Tips voor als het misgaat

- Controleer of iedereen in het team hun toegewezen groepsnummer gebruikt.
- Zorg ervoor dat de ontvanger en hacker hun programma's uitvoeren en wachten voordat de zender het bericht verstuurt.
- Zorg ervoor dat de zender en ontvanger dezelfde sleutel gebruiken.
- Zorg ervoor dat de hacker de sleutel kent.