INSTITUTO POLITÉCNICO DE BEJA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

MESTRADO EM ENGENHARIA DE SEGURANÇA INFORMÁTICA

CRIPTOGRAFIA E CRIPTOANÁLISE APLICADAS

EXERCÍCIOS EM PYTHON

Versão 2122-a
[7 de dezembro de 2021]

Prof. Daniel Franco

Laboratório UbiNET – Segurança Informática e Cibercrime

A. Preparação do ambiente de programação em Python:

    a. Download de: www.python.org versão 3.10.0;
    b. Instalação “Custom” com a adição do Python ao PATH;
    c. Escolher o local de instalação “c:\Python3100\;
    d. Instalar para todos os utilizadores e “precompile standard library”;
    e. “Disable path length limit”;
    f. Abrir o Python IDLE;
    g. Crie um novo ficheiro;
    h. Teste a instalação com um pequeno programa de “Hello World”.

1. O que entende por criptanalise?

2. Argumente sobre ataques por criptanalise.

3. Recorrendo à linguagem de programação Python, desenvolva um programa com uma função que permita cifrar uma String através da Cifra de César:

    a. Cifre a mensagem “BEJA” com chave 2;
    b. Cifre a mensagem “XPTO” com chave 12;
    c. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

4. Recorrendo à linguagem de programação Python, desenvolva um programa com uma função que permita cifrar uma String através da Cifra Play Fair:

    a. Cifre a mensagem “PORTUGAL” com a chave “BENFICA”;
    b. Cifre a mensagem “RUSS BALLARD” com a chave “DREAM ON”;
    c. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

5. Recorrendo à linguagem de programação Python, desenvolva um programa com uma função que permita cifrar uma String através da Cifra Vigínere:

    a. Cifre a mensagem “THE FIRE” com a chave “BALLARD”;
    b. Cifre a mensagem “MUNDO” com a chave “ALENTEJO”;
    c. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

6. Recorrendo à linguagem de programação Python, desenvolva um programa com uma função que permita cifrar uma String através da Cifra Rail-Fence:

    a. Cifre a mensagem “PORTUGAL” com dois vetores de 4 posições cada;
    b. Cifre a mensagem “FELICIDADE” com 2 vetores de 3 posições cada;
    c. Cifre a mensagem “WHITESANVIR” com 3 vetores de 4 posições cada;

d. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

7. Altere o programa desenvolvido no exercício 3 para incluir uma função de decifra de uma String cifrada com a Cifra de César:

    a. Decifre o criptograma “ANAF” com chave 5;
    b. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

8. Altere o programa desenvolvido no exercício 4 para incluir uma função de decifra de uma String cifrada com a Cifra Play Fair:

    a. Decifre o criptograma “ENFIBHDW” com chave “BENFICA”;
    b. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

9. Altere o programa desenvolvido no exercício 5 para incluir uma função de decifra de uma String cifrada com a Cifra Vigínere:

    a. Decifre o criptograma “Q0T” com chave “PORTUGAL”;
    b. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

10. Altere o programa desenvolvido no exercício 6 para incluir uma função de decifra de uma String cifrada com a Cifra Rail-Fence:

    a. Decifre o criptograma “WHITEASANVIR” com 3 vetores de 4 posições cada;
    b. Compare os resultados com os resultados obtidos na ficha de exercícios de criptografia.

11. Tendo como referência a análise de frequências, desenvolva um programa em Python que seja capaz de quebrar a Cifra de César:
    a. Explique como funciona a análise de frequências e como esta pode ser aplicada para quebrar a Cifra de César;
    b. Descubra a mensagem original tendo como fonte o seguinte criptograma:

        “fdrijrcxrufhlrekfufkvljrcjrfcrxizdrjuvgfiklxrcgfikvtilqridfjhlrekrjdrvjtyfirirdhlrekfjwz cyfjvdmrfivqrirdhlrekrjefzmrjwztrirdgfitrjrigrirhlvwfjjvjefjjffdrimrcvlrgverklufmrcvr gverjvrrcdrerfvgvhlverhlvdhlvigrjjrircvdufsfarufikvdhlvgrjjrircvdurufiuvljrfdrifgvizxf vfrszjdfuvldrjevcvvhlvvjgvcyflftvl”

    c. Qual foi a chave utilizada para cifrar o criptograma anterior? Explique porque é que a chave utilizada não é a chave que se estaria à espera, de acordo com a análise de frequências?

12. Desenvolva um programa em Python que permita a realização de um ataque de força bruta à Cifra de César:
    a. Encontra a chave de cifra utilizada para cifrar o seguinte criptograma:

       "aymdemxsmpacgmzfapafqgemxemaxmsduymepqbadfgsmxbadfqodglmdyaecg mzfmeymqeotadmdmycgmzfaeruxtaeqyhmadqlmdmycgmzfmezauhmeruomdmy badomemdbmdmcgqraeeqezaeeaaymdhmxqgmbqzmfgpahmxqmbqzmeqmmxy mzmaqbqcgqzmcgqycgqdbmeemdmxqypanavmpadfqycgqbmeemdmxqypmpadp qgemaymdabqdusaqamnueyapqgymezqxqqcgqqebqxtagaoqg"

    b. Explique como funciona o ataque de força bruta à Cifra de César

13. Tendo como base a análise de frequências, desenvolva um programa em Python que seja capaz de quebrar a Cifra de Vigenére:
    a. Sabendo que a chave de cifra utilizada tem comprimento 10, descubra a mensagem escondida no criptograma:

       "atmejaoheharbwmaumscqqcwoyhjqdypwvypintndeutidadrbanamghegssqmxgiz onwnyetzidagmlqnbgmqmhicudiioqoxsmteignqmksbanbmxanjwrabmexqmvmnd gzshpeuematmewamzsmatmezumpqoamwwrfixspgevgjadzwddrmhudtdhnbolwh pozrsdebshfokvnhazsnadjqtzdwghupmirqnbwifehtnqsbwgfuysnqqcafnrdscmvqvu pekimpemkmqnxmzxmmfnqdzwsqbmemgpmilaeymyysjyaqrkggmczvsaaymuztdh zpelwpmgvvngalwyepzvzcumkypeqiodnikwainerzokgldeiymoawjcecjennuauudpjv dxaavypeavnztijmqcjqncumfibomutqsiboetvqdpilsxatzqoadiboetvrzfuzwtmdvwba iasm"

    b. Utilize o método de Kasiski para encontrar o comprimento da chave de cifra utilizada para cifrar o criptograma:

       "atmebowemiwjfeaggrwvqqcwgmpgyeuhadmvusxgdeutariazcwfeuunqlwlqmxga nwkeouwxhwjmlqeqnbgeeueqdqvmqcwacwfteigfeuhacwffulgzoakabmepeusuozy davvqzifatmeoouwanwlqmnayuuhamwwjtquaqcwzoxgpeawdrmhmrbapoxgpevv aevldebsztwhdodsdabgpoumzdwgzixjqsmffewlqmxgqsbwytcvaomigittdiwvmvqv mdmhqnlwqsawzcqsxmmffelwetmtqmambrmeaeymqmaggbmjoousoezlaaymmn bapalwpedssazggalwqsxwdaymqsmvqvmhdnikooqkmsvgoozjqncfoawjuskgmojm ecijbozwxaavqdmxdovlmrawoougcumfapwjcumkmjckfauwpilspobwypwvmjckfav sfuzwlalsecwaeaa"

14. Recorrendo à Cifra Affine, cifre a seguinte mensagem, tendo como base a chave a=7 e b=2:

    "a disciplina de CCA terminara no final de janeiro do ano de dois mil e vinte e dois"

15. Desenvolva um programa em Python que permita cifrar e decifrar mensagens com recurso à Cifra Affine:
    a. Cifre a mensagem do exercício 14 e compare com os resultados obtidos anteriormente

16. Como poderá ser quebrada a Cifra Affine? Desenvolva um programa em Python que permita quebrar esta cifra. Utilize exemplos e descreva os resultados.

17. Investigue o perigo do ataque Man-in-the-Middle em comunicações com chaves assimétricas.

Nota: Todas a mensagens utilizadas nestes exercícios estão escritas em Português, utilizando-se o alfabeto expandido de 26 letras.

Boa Sorte!