Universidade Federal do Rio Grande do Sul – UFRGS

Professor: Weverton Cordeiro

Aluna: Marília de Matos Biz

Decriptação do Arquivo “arquivo-weak-7.in-full.hex”

A implementação utilizada foi ataque de força bruta, com algumas informações conhecidas.

1ª Informações conhecidas são:

- A chave inicia com SecurityAESXXXXX
- O Algoritmo usado é o AES no modo ECB
- O texto decifrado é legível em ASCII

2º O restante da chave é gerado combinando letras e dígitos (string.ascii_letters + string.digits) em todas as possibilidades para o comprimento desconhecido.

3º Resultado do arquivo decriptado:

Chave fraca encontrada: SecurityAESg1n8T

Texto decifrado: Cras scelerisque pellentesque lectus, quis varius risus varius non. Fusce eu augue at ante bibendum mollis. Quisque accumsan dapibus purus, id sodales dolor. Morbi feugiat tristique facilisis. Maecenas nisl velit, gravida et nisl mattis, euismod interdum lacus. Quisque et est iaculis, malesuada tortor eget, dignissim justo. Nulla ut sodales ex. Suspendisse at vestibulum velit. In hac habitasse platea dictumst. Proin facilisis faucibus tellus, vitae sodales est porta sit amet. Nullam eget accumsan dolor. In feugiat nunc sed nunc pretium, non bibendum ante condimentum. Vestibulum ac ultrices nisl. Praesent arcu tortor, vestibulum et dolor in, pretium sollicitudin ipsum. Maecenas vitae ipsum quis ligula sagittis egestas quis ut mauris. Mauris lacus metus, accumsan sit amet consequat id, rutrum vel neque. Nunc accumsan laoreet justo. In hac habitasse platea dictumst. Nullam viverra, tellus ullamcorper mattis vulputate, lectus mauris aliquam justo, a ultricies felis ipsum ut tellus. Maecenas ac dui non diam malesuada posuere. Cras lorem est, molestie at est nec, varius tempor est. Cras maximus maximus nunc. Aliquam sagittis metus id maximus laoreet. In eget neque at nisl ultricies ornare vitae ut leo. In vulputate nisl ut velit tempus, eget facilisis massa tempus. In sit amet lorem vitae lorem aliquam tempor. Sed in libero ullamcorper risus ultricies venenatis non nec risus. Phasellus bibendum dolor ut nibh dapibus egestas. Vivamus eu enim luctus, blandit augue in, pellentesque nisl. Pellentesque velit eros, malesuada nec varius ac, dictum eget ligula. Ut sed ipsum pharetra...

Parabens! Codigo secreto: DPX4at

Decriptação do Arquivo “arquivo-strong-7.in-full.hex”

A implementação utilizada foi ataque de força bruta, com algumas informações conhecidas.

1ª Informação conhecida critica:

- A chave começa com "Security00".
- O algoritmo usado é o AES no modo ECB.
- O texto decifrado pode ou não estar legível em ASCII.

2º Não foi realizado testes de chaves, foi apenas convertido de hex para utf-8

3º Resultado do arquivo

Não possui chave

Lórém ipsûm dólor sit amet, consectetur adipiscing elit. Sed mauris massa, pulvinar et accumsan condimentum, rutrum fringilla justo. Integer hendrerit leo volutpat malesuada venenatis. Vivamus euismod viverra erat, eu fermentum nisi viverra nec. Quisque pharetra venenatis libero, id mollis neque consectetur at. Mauris venenatis lorem at dictum sodales. Nam sed nisi eu metus maximus pharetra vitae tincidunt risus. Nullam urna quam, sagittis eget congue at, luctus nec lorem. Integer hendrerit imperdiet augue ac semper. Vestibulum varius fermentum eleifend. Duis vitae tellus pharetra, luctus libero vel, luctus ipsum. Morbi tempor ornare nibh in viverra. Duis molestie dapibus libero vel consequat. Donec vitae malesuada magna. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nullam pretium turpis eu commodo faucibus. In finibus, erat quis rhoncus sodales, sapien enim posuere neque, id egestas velit sem nec nulla. Pellentesque ipsum magna, venenatis id eleifend a, accumsan eu lorem. Aliquam erat volutpat. Sed ut ultricies neque, a egestas mi. Pellentesque pellentesque, justo id varius vestibulum, enim risus euismod augue, et suscipit neque elit eget magna. Nam tempor sit amet lacus id volutpat. Donec egestas faucibus mauris. In molestie tincidunt mi. Mauris scelerisque, tortor vel pharetra sagittis, tellus velit pharetra erat, a ultricies ex risus tempor felis. Cras condimentum ac erat eu convallis. Nulla sapien ipsum, ullamcorper in interdum at, consectetur vitae quam. Phasellus ligula mi, scelerisque sit amet lacus nec, lacini..

Êxito na força bruta:: 4Cgh3y