Segurança em Sistemas de Computação

Desafio 04

INF01045 – Segurança em Sistemas de Computação – Turma U – Prof. Raul Weber

Luiz Gustavo Frozi de Castro e Souza - Cartão 96957
Mário César Gasparoni Jr. - Cartão 151480

Setembro de 2013

Texto:

AANACOBSHENITMAONDFMESENMURBHESCOCOURAELETIANUIPLGNCSHINSMTGNUTEESDAAOTUSLSNIAEENATHHIENM
GVFTRUSEEFHEIOTLSANAPPAANTBNAANTTILEULSRCAPTEILVIARDRMFHORUIYIFRTERAONDROTTEPFRHUOCTBEDOF
IINFASNDENRRAMAONAALPEYTTTHLNSRTENTRAVTOAIEPLICEAOOTHASUTAERTASIBUNSAEEWITIRYULDLCAITEICV
TOPDNRLIRECAANBEGOSSTEOIZUERSFHIATNDREEUTUSRCAANASABLNTNPAEEOFAKRMSTTNINTFOHEEESTRREAANAG
RBRITNFUWAINCLOGNGHNISSTEPTUIHURWTTTWETTOFUINYRARTIREONTHEADTEOTERETTIWNYTUOACHSCEABNHNID
IANIULBVDANSAHECAPOTAARIUVEYETELAOTRWAITYERLSHHFEIIBLORDNRPENEIAONARTAASBNNAUVAOUEBESLALC
VEONARTMIFIADAPOBANSUMTSIAANAWNNEROSRGNHONDAINREEUDDRTHCONYWOITTNETRDWUWRLISODREMANITANOE
HORTHCRYRITEFUPABAMEOACONNSNRAVFSIEYOAITZNESRSICLOADOOUSTRSMTVACLIRLEYENAOWHELWIHPEFRRRPE
TEIIETIPEUSLYSAILNEDNREETEADAWOORHIAKDTCOETWEXRASSXTTAETREDWICMHEFOTIIPEHEKFRTDAOICFTGRFY
TOHRPPCHINGAALECHLYIOUDTELEEWLNIEMPREOETALMNUBCEORDUEFDRTEAATINCKGATCATXATYPSECRETNETDWDV
TTEAIHHNECETIACYPDNRNOALOROIHMGRTERSFINAHRTOSOHEEEICTTONLCROODEEOCKODBOMEOCBTBRSORFRHTHWI
EKUUTHTOTODWLHENEFTEGOOSRRNGCODIEPNLTAIUSPXYONETOBULTOHALEDEBNZALINAATRYESOTFBFIGSNDYEADY
AWTINFISAODGHUIENNEWESBTAMNDRIRIBEOGBHAANENSOERDCHPSHRTETWITAERIRNPSENUUEOTGFPPBOOHMNMEDC

Texto Decifrado:

banana is the common name used for herbaceous cultigenic plants in the genus musa and is also the name given the fruit of these plants banana plants are cultivated primarily for their fruit and for the production of fiber and as ornamental plants they are native to tropical south eastern asia but are widely cultivated intropical regions because of their size and structure banana plants are often mistaken for trees the banana fruit grow in hanging clusters with up to twenty fruit to a tier and three to twenty tiers to a bunch each individual banana has a protective outerlayer with a fleshy edible inner portion bananas are a valuable source of vitamin and potassium bananas are grown in one hundred and thirty two countries world wide more than any other fruit crop bananas come in a variety of sizes and colors most cultivars are yellow when ripe the ripe fruit is easily peeled and eaten raw or cooked this text was extracted from the wikipedia for the fifth cryptographic challenge you will need to implement a reduced brute force attack against a text encrypted with the advanced encryption algorithm or aes for short in the electronic code book mode or ecb for short but without the knowledge of the corresponding plaintext you should be able to analyze a string of bytes and find a way of distinguish between random gibberish and a coherent phrase written in portuguese hfpbepdmcnmoo

Chave de Identificação: FPPBOOHMNMEDC => hfpbepdmcnmoo

Colunas: 13

Chave de Permutação: ABCDEFGHIJKLM => gacdkblhmijef

Passo a Passo da Análise Efetuada:

1. Dica: "uses permutation"
2. Dica: "the text fits perfectly in a rectangular area"
3. Fatores de size(M) = 1157: { 1, 13, 89, 1157 }
4. Dica: "the number of rows is greater than the number of columns"
5. Juntando todos os passos anteriores, podemos dizer que a transposição foi efetuada usando 13 colunas
6. Dica: "word banana appears several times"
7. Procurar organizar as trocas para formar a palavra "banana"
8. Análise de frequência: e = 11,41%, t = 9,77%, a = 9,77%
9. Com base na análise de frequência podemos dizer que o texto está em Inglês
10. Reordenar colunas para aumentar a legibilidade do texto, procurando elementos como “and” e “the”.