# Segurança em Sistemas de Computação

*Desafio 02*

*INF01045 – Comunicação – Turma U – Prof. Raul Weber*

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

*Agosto de 2013*

**Texto:**

VS XERMGKOETZRT, JST XRZET UV QJBQGRGJRXTK V JS SVGKUK UV XERMGKOETZRT FJV KMVET UV TXKEUK XKS JS QRQGVST MEV-UVZRARUK UV QJBQGRGJRXTK. MTET XERMGKOETZTE JST SVAQTOVS, JARUTUVQ UK GVYGK - FJV MKUVS QVE PVGETQ RQKPTUTQ, MTEVQ KJ KJGEKQ OEJMKQ UV PVGETQ - QTK QJBQGRGJRUTQ MTET ZKESTE T XRZET. TQ XRZETQ UV QJBQGRGJRXTK QTK UVXRZETUTQ MVPT QJBQGRGJRXTK RAWVEQT. GKUTWRT, QV T JARUTUV UV QJBQGRGJRXTK VQGRWVE TK ARWVP UV MTPTWETQ RAGVRETQ KJ ZETQVQ, K QRQGVST V ITBRGJTPSVAGV URGK QVE JS XKUROK, ATK JST XRZET.

VYRQGVS URWVEQKQ GRMKQ UV XRZETQ UV QJBQGRGJRXTK. QV T XRZET KMVET XKS PVGETQ RQKPTUTQ, V UVAKSRATUT XRZET UV QJBQGRGJRXTK QRSMPVQ. QV KMVET XKS OEJMKQ UV PVGETQ XITST-QV XRZET UV QJBQGRGJRXTK MKPROETZRXT. JST XRZET SKAKTPZTBVGRXT JQT JST QK QJBQGRGJRXTK ZRYT AT SVAQTOVS RAGVRET, VAFJTAGK JST XRZET MKPRTPZTBVGRXT JQT STRQ FJV JST. JST XRZET MKUV TRAUT EVXKEEVE T IKSKZKAKQ FJTAUK JST JARUTUV UV GVYGK MKUV STMVTUT VS STRQ FJV JST MKQQRBRPRUTUV URQGRAGT.

T TATPRQV UV ZEVFJVAXRT ZKR T ZVEETSVAGT BTQRXT MTET FJVBETE XRZETQ XPTQQRXTQ. VS PRAOJTQ ATGJETRQ, UVGVESRATUTQ PVGETQ UK TPZTBVGK TMTEVXVS STRQ ZEVFJVAGVSVAGV UK FJV KJGETQ. MKE VYVSMPK, AJST XRZET QRSMPVQ UV QJBQGRGJRXTK (VS FJV XTUT PVGET V QJBQGRGJRUT QRSMPVQSVAGV MKE KJGET), T PVGET STRQ ZEVFJVAGV AJST SVAQTOVS XRZETUT UV JS GVYGK VS MKEGJOJVQ QVERT T FJV EVMEVQVAGT T PVGET "T".

T XERMGKOETZRT SKUVEAT GKEAKJ SJRGK STRQ XKSMPVYT T XERMGKTATPRQV UK FJV KQ QRQGVSTQ "MTMVP-V-XTAVGT" UK MTQQTUK, V MTEVXV TOKET QVE QJMVERKE T XERMGKTATPRQV. QVOJAUK K IRQGKERTUKE UTWRU CTIA, "SJRGKQ QTK KQ XERMGKQQRQGVSTQ KZVEVXRUKQ MVPTQ XVAGVATQ UKQ WVAUVUKEVQ XKSVEXRTRQ TGJTRQ FJV ATK MKUVS QVE FJVBETUKQ MKE FJTPFJVE SVGKUK XKAIVXRUK UT XERMGKTATPRQV".

CTIA MKUV GVE QRUK MEVSTGJEK VS QJT TATPRQV. TQ XRZETQ ZETXTQ ATK ZKETS VYGRAGTQ, V KQ SVGKUKQ XERMGTATPRGRXKQ VSMEVOTUKQ MKE TOVAXRTQ UV RAGVPROVAXRT MVESTAVXVS ATK MJBPRXTUKQ. AT TXTUVSRT, MEKLVGKQ AKWKQ QTK TMEVQVAGTUKQ EVOJPTESVAGV, V GTSBVS FJVBETUKQ ZEVFJVAGVSVAGV. AT RAUJQGERT, GTSBVS, XRZETQ ATK QTK PRWEVQ UV ZTPITQ: MKE VYVSMPK, KQ TPOKERGSKQ JQTUKQ AT GVXAKPKORT UV GVPVZKAV XVPJPTE MKUVS QVE FJVBETUKQ VS IKETQ KJ SRAJGKQ. K MEKGKXKPK NREVU VFJRWTPVAG MERWTXD (NVM), JQTUK MTET T QVOJETAXT UV EVUVQ NR-ZR, ZKR FJVBETUK MKE JS TGTFJV METGRXK UV XITWV EVPTXRKATUT. VQQT ZETFJVHT ATK VET EVTPSVAGV UK TPOKERGSK VS QR, STQ MERAXRMTPSVAGV UVWRUK TK QVJ JQK RSMEKMERK UVAGEK UK MEKGKXKPK, UV SKUK T XKSMEKSVGVE QJT ZKEXT.

QV WKXV UVXRZEKJ K GVYGK XKS QJXVQQK, QTRBT VAGTK FJV K GVEXVREK UVQTZRK QVET VQXERGK VS RAOPVQ V FJV XKAGVS T MTPTWET XEDMGKOETMID.

WEXAYQFHEEJSVUAHWQYMYRTGUR

**Texto Decifrado:**

*em criptografia, uma cifra de substituicao e um metodo de criptografia que opera de acordo com um sistema pre-definido de substituicao. para criptografar uma mensagem, unidades do texto - que podem ser letras isoladas, pares ou outros grupos de letras - sao substituidas para formar a cifra. as cifras de substituicao sao decifradas pela substituicao inversa. todavia, se a unidade de substituicao estiver ao nivel de palavras inteiras ou frases, o sistema e habitualmente dito ser um codigo, nao uma cifra.*

*existem diversos tipos de cifras de substituicao. se a cifra opera com letras isoladas, e denominada cifra de substituicao simples. se opera com grupos de letras chama-se cifra de substituicao poligrafica. uma cifra monoalfabetica usa uma so substituicao fixa na mensagem inteira, enquanto uma cifra polialfabetica usa mais que uma. uma cifra pode ainda recorrer a homofonos quando uma unidade de texto pode mapeada em mais que uma possibilidade distinta.*

*a analise de frequencia foi a ferramenta basica para quebrar cifras classicas. em linguas naturais, determinadas letras do alfabeto aparecem mais frequentemente do que outras. por exemplo, numa cifra simples de substituicao (em que cada letra e substituida simplesmente por outra), a letra mais frequente numa mensagem cifrada de um texto em portugues seria a que representa a letra “a”.*

*a criptografia moderna tornou muito mais complexa a criptoanalise do que os sistemas “papel-e-caneta” do passado, e parece agora ser superior a criptoanalise. segundo o historiador david kahn, “muitos sao os criptossistemas oferecidos pelas centenas dos vendedores comerciais atuais que nao podem ser quebrados por qualquer metodo conhecido da criptoanalise".*

*kahn pode ter sido prematuro em sua analise. as cifras fracas nao foram extintas, e os metodos criptanaliticos empregados por agencias de inteligencia permanecem nao publicados. na academia, projetos novos sao apresentados regularmente, e tambem quebrados frequentemente. na industria, tambem, cifras nao sao livres de falhas: por exemplo, os algoritmos usados na tecnologia de telefone celular podem ser quebrados em horas ou minutos. o protocolo wired equivalent privacy (wep), usado para a seguranca de redes wi-fi, foi quebrado por um ataque pratico de chave relacionada. essa fraqueza nao era realmente do algoritmo em si, mas principalmente devido ao seu uso improprio dentro do protocolo, de modo a comprometer sua forca.*

*se voce decifrou o texto com sucesso, saiba entao que o terceiro desafio sera escrito em ingles e que contem a palavra cryptography.*

*vrcnxsqzrrumednzvsxpxiatdi*

**Chave:**
WEXAYQFHEEJSVUAHWQYMYRTGUR => vrcnxsqzrrumednzvsxpxiatdi

**Tabela de Substituição Usada:**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| n | b | k | y | r | q | t | z | h | u | o | j | p | w | g | l | s | i | m | a | d | e | v | c | x | f |