

Aluno(a):			RA:
Curso	Análise e Desenvolvimento de Sistemas	Semestre: 5	
Disciplina	Segurança da Informação		Nota da Avaliação:
Professor	Adriano Ricardo Ruggero		
Tarefas			Rubrica do Professor
Orientações gerais:			
1 - Todos os trabalhos devem ser realizados individualmente			
2 - Submeta suas respostas/arquivos no endereço https://goo.gl/BmIUPJ			
3 - Os arquivos devem estar em formato PDF .			
4 - Data limite para submissão das respostas/arquivos: 29/06/2017 .			

- (2 ½ Pontos) Analise o caso do *Morris Worm* (1988) e explique com riqueza de detalhes.
- (2 ½ Pontos) Escreva um ensaio sobre o “Ovo do Cuco” (*Cucckoo’s Egg*), que envolveu Cliford Stoll no que foi considerado o primeiro caso documentado de resposta a um incidente e detecção de invasão.
- (2 ½ Pontos) Escreva um ensaio sobre “ataques de amplificação” (*amplification attacks*), ou seja, ataques que usam um servidor (vítima) para gerar mais dados que os recebidos do atacante original. Tais ataques são arquitetados de tal forma que não retornam os dados ao atacante, mas a outra vítima, com a intenção de causar DoS.
- (2 ½ Pontos) **Desafio!!!** O texto cifrado a seguir foi encriptado usando uma cifra de substituição. Decripte o texto cifrado sem conhecer a chave. Obs.: o texto está em **inglês** (o que não deve ser problema para vocês):

lrvnmnr bpr sumvbvwr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjjudwko bj yt wkbrusurbmbwj k lmird jk xjubt trmui jx ibndt wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrk mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjysrbr rashmkmbwj k jk cjhnd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urv-jokw gwko i jnkdhr ii jnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj dnlb bpmb bpr xjhhjcwko wi bpr sujsru mshwvmbwj k mkd wkbrusurbmbwj k wjxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmrv

- Calcule a frequência relativa de todas as letras (a, b, c...) no texto cifrado. Você pode querer usar uma ferramenta como o programa *Cryptool* (<https://www.cryptool.org/en/>) para fazer isto. Entretanto, usar lápis e papel também é factível.
- Decripte o texto cifrado com ajuda da frequência relativa das letras da língua inglesa (veja a Tabela 1.1 na Seção 1.2.2 do livro *Understanding Cryptography*, disponível no [link https://goo.gl/BmIUPJ](https://goo.gl/BmIUPJ)). Atente que este texto é relativamente curto, então a frequência de letras pode não estar perfeitamente alinhada com a tabela do livro.
- Quem escreveu o texto?