Universidade Tecnológica Federal do Paraná (UTFPR) Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia (IF6CL)

Professor: Rodrigo Minetto (rminetto@dainf.ct.utfpr.edu.br)

Lista de exercícios

- 1) Codifique o algoritmo RSA e teste-o com os seguintes dados:
- p = 11, q = 13, e = 7. Qual a chave privada? Qual a chave pública? Qual o valor cifrado com esses dados se o texto em claro for x = 9? Solução: $k_{pub} = (7, 143)$, $k_{priv} = (103, 143)$ e texto cifrado = 48.
- p = 7, q = 19, e = 5. Qual a chave privada? Qual a chave pública? Qual o valor cifrado com esses dados se o texto em claro for x = 6?
- p = 17, q = 11, e = 7. Qual a chave privada? Qual a chave pública? Qual o valor cifrado com esses dados se o texto em claro for x = 88?
- 2) Sejam dois primos p = 41 e q = 17 utilizados como entrada no RSA. Qual valor $e_1 = 32$ ou $e_2 = 49$ é um expoente válido para o RSA? Justifique sua escolha. Qual a chave privada que resulta da escolha do expoente correto?
- 3) Suponha que você recebeu o seguinte texto cifrado y = 1141, por meio de um espião através de uma conexão monitorada. A chave pública utilizada foi $k_{pub} = (e, n) = (2111, 2623)$. Qual o texto em claro x?
- 4) Suponha que você recebeu o seguinte texto cifrado y = 1632643, por meio de um espião através de uma conexão monitorada. A chave pública utilizada foi $k_{pub} = (e, n) = (5, 6326693)$. Qual o texto em claro x?