Teoria de Informação
Ficha Teórico-Prática nº3

"Criptografia"

Período de execução: 1 semana
Objectivo: Pretende-se que o aluno adquira sensibilidade para as questões relacionadas com a encriptação.

Trabalho

1. Resolva os seguintes problemas:
   a. Seja x = 17 mod 11 e y = 13 mod 11. Determine xy mod 11, (x+y) mod 11 e (x-y) mod 11.
   b. Determine o mdc(30030, 257).
   c. Encontre os inteiros x e y, tal que 17x+101y=1.
   d. Encontre os inteiros x e y, tal que 172x+190y=mdc(172, 190).
   e. Determine a solução da equação 7x mod 30 = 1.
   f. Determine 2^{1234} mod 789.

2. Considere n = 7 e m= 15. Determine uma solução simultânea x mod 7 = 3 e x mod 15 = 5.

3. Se n=221 e o resultado da função de Euler for 192, determine p e q.

4. A cifra 5859 foi obtida usando RSA com n = 11413 e e = 7467. Usando a factorização n = 101 x 113, determine a mensagem.

5. Suponha que num esquema RSA n= 55 = 5 x 11 e que e = 3.
   a. Determine d.
   b. Assuma que mdc (m, 55)=1. Mostre que se $c=m^3$ mod 55 é o texto da cifra, então m = c^d mod 55.

6. Suponha que a mensagem *m* = 5575 deve ser encriptada usando RSA.
   a. Considere que deve escolher os primos *p* e de *q* tal que *p* e *q* sejam menores que 7500. Estime o número de números primos inferiores a 7500.
   b. Determine dois números primos entre 4000 e 7500. Observe que não deverá factorizar os números para determinar se são primos.
   c. Determine a função de Euler do número *n* = *pq*.
   d. Determine um expoente *e* maior que 100.
   e. Determine um expoente *d* adequado.
   f. Encripte a mensagem *m.*
   g. Desencripte a mensagem cifrada obtida em f.

7. Seja p = 7919 e q = 17389. Seja e = 66909025. Observa-se que e^2 mod (p-1)(q-1) = 1. Considerando que a mensagem é m = 12345, qual será o resultado da cifra se houver duas encriptações consecutivas com a chave (n,e)?