Verifica di SISTEMI e RETI, classe 5^A ROB.

Crittografia ed algoritmo RSA

Dati p = 13 e q = 19 e ponendo c = 41:

1. generate la chiave pubblica dell'algoritmo crittografico RSA
2. generate la chiave privata dell'algoritmo crittografico RSA
3. auto-valutate la vostra verifica con un punteggio x compreso tra 1 e 10, successivamente crittografate il numero x+10 usando la chiave privata ottenuta al punto 2.

4. Enunciate il principio di Kerckhoffs e spiegatene il significato.
5. Descrivete i vantaggi degli algoritmi crittografici asimmetrici rispetto a quelli simmetrici.

NOTA: per ognuno dei punti 1,2,3 scrivere i risultati e tutti i passaggi intermedi o eventuali spiegazioni qualora necessarie. Nel caso si indichino soltanto i risultati, l'esercizio sarà considerato completamente errato.

ES 1-2-3

p= 13

q=19

c=41

- **1 : CALCOLARE LA CHIAVE PUBBLICA**

n=(p*q)=13*19=247

n e c compongono la chiave pubblica

(247, 41)

- **2 : CALCOLARE LA CHIAVE PRIVATA**
  (CALCOLI SU FOGLIO DA QUA IN AVANTI)

m= mcm(12,18)
m= (12*18)/mcd(12,18)
m= 216/ 6 = 36 → prima parte chiave privata

la seconda parte è d
c*d-k*m=1
d= 29 (calcoli sul foglio)

m e d compongono la chiave pubblica
(36, 29)

- **3 : CALCOLARE VOTO**
  x= 7
  x+10=17

  (17)^41 mod 247 = 131 (calcoli sul foglio)

- **4: ENUNCIARE IL PRINCIPIO DI KERCKHOFFS**
  Il principio di Kerckhoffs afferma che la sicurezza di un sistema di crittografia sta nella sicurezza della chiave e non nell'algoritmo. Ciò implica che nel caso di un attacco l'algoritmo può anche essere scoperto e violato ma l'importante è che si renda pubblica la chiave. Riassumendo, secondo Kerckhoffs : chiave sicura → crittografia sicura

- **5 : SPIEGARE I VANTAGGI DEGLI ALGORITMI SIMMETRICI VS QUELLI ASIMMETRICI**
  La sicurezza di un algoritmo asimmetrico sta nel fatto che le chiavi presenti sono due: 1 pubblica e 1 privata. Questa caratteristica permette all'algoritmo di essere molto sicuro e forte in quanto anche avendo la possibilità di "leggere" la chiave pubblica, la chiave privata (che conosce solo il destinatario) rimarrà segreta e unilaterale. Al contrario, negli algoritmi simmetrici la chiave pubblica è una sola e una volta a conoscenza della stessa si riesce a decifrare il messaggio in modo pressoché semplice eseguendo un attacco di tipo man in the middle .

FOTO DEI CALCOLI DEGLI ES 1-2-3

YURI ARMANDO - CALCOLI VERIFICA SISTEMI

mcd = 6

18	12
12	6
0	0

→ mcd = 6

d = →

41	36
36	5
35	1

$1 = 36 - (5 \cdot 7) = 36 - [7(41 - 36)] =$

$= 36 - [7 \cdot 41] + (7 \cdot 36)] = (8 \cdot 36) - (7 \cdot 41)$

$c \cdot d \bmod m = 1$

$41 \cdot d \bmod 36 = 1$

$41 \cdot d = 1 + 36 \cdot k$ → FORMULA TRAC

$41 \cdot d - 36 \cdot k = 1$

$41 \cdot (-7) - 36 \cdot k = 1$

DA PORTARE POSITIVO

QUINDI

$-7 + 36 = \boxed{29 \quad d}$

3 CRITTOGRAFA IL 20

$b = (17^{41}) \bmod 247$

$(17^5 \bmod 247)^7 \; (17^6 \bmod 247)^{\bmod 247} =$

$= [5748 \cdot 247]$

↓

SOTTRATTO A 17^5 DA 113

↳ resto

↓

$113 + 7 = \boxed{833}$

$17^6 \bmod 247 = 235$ → CALCOLATRICE

$235 \; 833 \bmod 247 = \boxed{131}$

↓

MESSAGGIO CRITTOGRAFATO