# Rezolvări - Criptografie (RSA, AES, DDH)

## 1. RSA - Chei și Decriptare

Fie p = 41, q = 17.  
  
- φ(n) = (p - 1)(q - 1) = 40 \* 16 = 640  
  
(a) Testăm e ∈ {32, 49, 5}  
- gcd(32, 640) = 32 ❌  
- gcd(49, 640) = 1 ✅ → valid  
- gcd(5, 640) = 5 ❌  
  
Răspuns: e = 49 este valid.  
  
(b) Calculăm d ≡ e^(-1) mod φ(n)  
- d = 393  
- Verificare: (393 \* 49) % 640 = 1

## 2. RSA - d pentru chei date

p = 31, q = 37, e = 17  
φ(n) = (p - 1)(q - 1) = 30 \* 36 = 1080  
d = e^(-1) mod 1080 = 953

## 3. AES - Runda completă

Pașii unei runde AES:  
1. AddRoundKey: XOR între statul inițial și cheia de rundă.  
2. SubBytes: Înlocuire fiecare octet cu valoarea din S-Box.  
3. ShiftRows: Rotirea rândurilor la stânga.  
4. MixColumns: Transformare lineară pe coloane în GF(2^8).  
  
Ieșirea finală după o rundă completă AES:  
[[165, 32, 71, 133],  
 [ 48, 49, 10, 128],  
 [ 20, 62, 178, 44],  
 [233, 209, 75, 39]]

## 4. Sisteme de criptare pe grupuri (DDH)

Criptarea unui bit b ∈ {0,1}:  
- b = 0: (c1, c2) = (g^y, h^y)  
- b = 1: (c1, c2) = (g^y, h^z), z ≠ y  
  
(a) Decriptare dacă știm x:  
- h = g^x ⇒ h^y = g^{xy}  
- Verificăm dacă c2 == c1^x ⇒ b = 0, altfel b = 1  
  
(b) CPA-securitate dacă DDH e greu:  
- Dacă adversarul nu poate distinge (g^y, h^y) de (g^y, h^z),  
 atunci sistemul este CPA-securizat.