# Criptografie și securitate CTI

## Laborator 9 - Problema logaritmului discret

### Protocolul de schimb de chei Diffie-Hellman

1. Jucați pe rând rolurile lui Alice și Bob în protocolul de schimb de chei Diffie-Hellman folosind următoarele numere $p = 3803$, $g = 2$, $a = 2704$, $b = 2023$, Verificați dacă la final Alice și Bob au aceeași cheie.

2. Repetați scenariul anterior considerând că Eve execută un atac de tipul *Man in the middle* cu $e = 1001$. Care este consecința acestui tip de atac?

3. Considerăm o variantă a protocolului de schimb de chei Diffie-Hellman în care înlocuim înmulțirea cu adunarea. Rămâne protocolul astfel definit sigur? Argumentați.

### Criptosistemul ElGamal

Link suplimentar: `https://www.studocu.com/ro/document/universitatea-politehnica-din-bucuresti/criptografie-si-criptanaliza/criptografie/28993831` - pg 163

4. Criptare și decriptare

   Cheia publică a destinatarului este $(p = 2579, \alpha = 2, \beta = 2400)$ iar cheia sa privată este $a = 123$.

   (a) Criptaţi mesajul 1324 folosind $k = 853$.

   (b) Decriptaţi mesajul $(y_1, y_2) = (1580, 342)$. Ce observaţi?

5. Utilizarea multiplă a lui $k$

   Cheia publică a lui Bob este $(p = 23, \alpha = 2, \beta = 18)$.

   (a) Oscar interceptează mesajul criptat $(y_1, y_2) = (13, 19)$ pe care Alice îl trimite lui Bob şi ştie că acestuia îi corespunde mesajul clar 7.

   Oscar interceptează apoi mesajul $(y_1', y_2') = (13, 9)$ pe care Alice îl trimite ulterior lui Bob.

   Oscar determină textul clar corespunzător celui de-al doilea mesaj. Care este acesta?

   (b) Care este greşeala făcută de Alice care îi permite lui Oscar să realizeze decriptarea?