*Lucrare individuală Nr. (… Criptografie….)*

*https://tools.ietf.org/html/rfc2631*

**Создание ключей с помощью экспоненциального алгоритма обмена ключами Диффи-Хеллмана**

Пусть два пользователя A, B.

A генерирует два числа: p = 11 простое число, g = 2, Zp, (*g - примитивный элемент*)

(De calculat cu Wolfram alpha: primitive root of 11 --- 2)

Ambii utilizatori aleg aleatory, in mod secret doua numere prime (obtinute prin teste de primalitate)

A are secretul **a = 5,**

B are secretul **b = 13.**

**Каждый пользователь вычисляет свой открытый ключ**

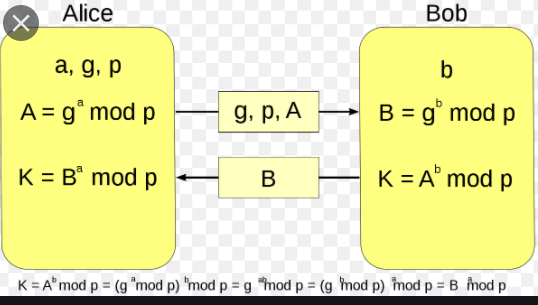
**A** calculeaza cheia publica: A = g a mod p = 25 mod 11 = **10** ---(restul de la impartirea la 11) este 10.

**B** calculeaza cheia publica: B= g b mod p = 213 mod 11 = **8.**

A, B fac schimb de chei publice pentru a calcula cheile secrete.

A calculeaza KA = 8 5 mod 11 = 10.

B calculeaza KB = 10 13 mod 11 = 10 => KA = KB. 10=10.

****

**Crearea cheilor cu algoritmul schimbului exponential de chei Diffie – Hellman**

INCEPUT

**Algoritmul schimbului de chei Difie-Helman**

Fie doi utilizatori A, B.

A genereaza doua numere: **p = 11** numar prim , **g = 2,** Zp, (*g-este element primitiv*)

Ambii utilizatori aleg aleatory, in mod secret doua numere prime (obtinute prin teste de primalitate)

A are secretul **a = 5,**

B are secretul **b = 13.**

**Fiecare utilizator isi calculeaza cheia sa publica**

**A** calculeaza cheia publica: A = g a mod p = 25 mod 11 = 10 ---(restul de la impartirea la 11) este 10.

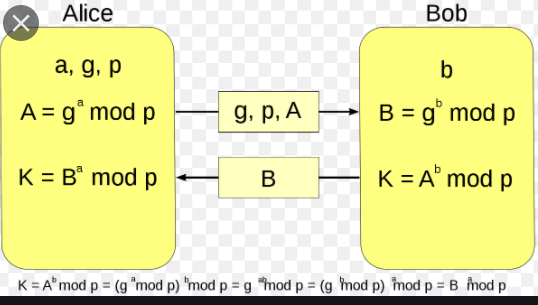
**B** calculeaza cheia publica: B= g b mod p = 213 mod 11 = 8.

A, B fac schimb de chei publice pentru a calcula cheile secrete.

A calculeaza KA = 8 5 mod 11 = 10.

B calculeaza KB = 10 13 mod 11 = 10 => KA = KB. 10=10.

**SFARSIT**

****