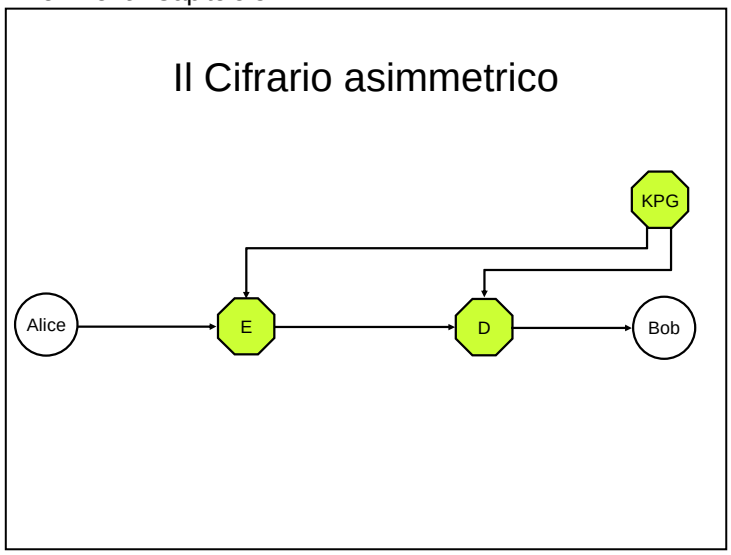
5. Esercitazioni consigliate

5.1 Il Cifrario asimmetrico

Obiettivo formativo – Analizzare il comportamento e valutare l'efficienza dei Cifrari RSA e ElGamal.
Riferimenti: Capitolo 5



Esperimenti:

1. Generare una coppia di chiavi per il Cifrario RSA. Generare un messaggio più piccolo del modulo. Esaminare e classificare il comportamento di RSA senza padding e con padding PKCS#1.
2. Prendere atto della dimensione del testo cifrato.
3. Prendere atto dei tempi di esecuzione della cifratura e della decifrazione. Fare un confronto con i tempi di esecuzione di un Cifrario simmetrico.
4. Trasportare la coppia di chiavi all'interno di un progetto dell'IDE ed impiegare il metodo "toString()" per analizzarne le componenti.
5. Generare una coppia di chiavi per il Cifrario di ElGamal. Generare un messaggio più piccolo del modulo. Esaminare e classificare il comportamento del Cifrario eseguendo due volte la cifratura senza padding.
6. Prendere atto della dimensione del testo cifrato.
7. Prendere atto dei tempi di esecuzione della cifratura e della decifrazione. Fare un confronto con i tempi di esecuzione di RSA.
8. Trasportare la coppia di chiavi all'interno di un progetto dell'IDE, ed estrarre le chiavi pubblica e privata effettuando un cast alle classi ElGamalPublicKey ed ElGamalPrivateKey di BouncyCastle. Impiegare il metodo "getParameters()" per ottenere, a partire dalle chiavi, un'istanza della classe ElGamalParameterSpec, da cui estrarre le componenti attraverso i metodi "getP()" e "getG". Stampare a video le componenti ed analizzarle.