

Leçon 11 : La cryptographie

Pour protéger le contenu d'un message, d'une conversation ou de données personnelles que l'on ne veut pas partager avec tout le monde il est parfois utile de rendre certains documents incompréhensibles des gens non destinataires.

Exemple :

Le message :

« **QLBKPK, H TPKP, KLZ YLUMVYAZ CPLUULUA WHY SH TLY** »

est un message incompréhensible qui permet de faire passer une information importante.

Le chiffrement est un procédé suivant lequel un document compréhensible de tous est transformé en un autre, incompréhensible.

Le déchiffrement est le procédé inverse.

Pour chiffrer un message, on utilise un algorithme de chiffrement. Très souvent les algorithmes de chiffrement s'appuient sur une clé de chiffrement. La clé utilisée pour chiffrer est parfois la même que la clé utilisée pour déchiffrer mais ce n'est pas toujours le cas.

