1:KNUMOTETE  
Le prime tracce note di crittografia si hanno col faraone egizio Knumotete II intorno al 1900 a.C. Sono stati infatti trovati alcuni geroglifici cifrati sulla sua tomba.

2.CESARE  
Intorno al 100 a.C. Giulio Cesare, per comunicare coi funzionari dell’esercito, usava dei messaggi cifrati. Egli sostituiva a ogni lettera del messaggio la lettera che la segue nell’alfabeto di 4 posti. Il suo cifrario venne chiamato cifrario di Cesare e si trattava di un cifrario a sostituzione monoalfabetico. Per convenzione si chiama cifrario di cesare ogni cifrario in cui una lettera venga sostituita con quella che la segue di N posti. Questo tipo di cifrari è molto debole in quanto la chiave può assumere solo 26 valori e sono quindi altrettanti i tentativi necessari per violare il cifrario.

3.VIGENERE  
intorno al 1600 Blaise de Vigenère sviluppò il primo cifrario polialfabetico. Le lettere del messaggio in chiaro non venivano infatti sostituite utilizzando la stessa chiave, ma si usava come chiave una parola chiamata “verme” che veniva scritta ripetutamente sotto al testo da cifrare e per cifrare una lettera bisognava sommare il suo numero d’ordine nell’alfabeto al numero d’ordine della lettera del verme corrispondente e poi riconvertire il numero trovato in lettera. È relativamente semplice da forzare se conosciamo la lunghezza della chiave e se questa è ignota si può procedere a tentativi impiegando un tempo discreto, grazie alla potenza dei calcolatori.

4.ENIGMA  
Durante la Seconda guerra mondiale i nazisti, per cifrare i propri messaggi, utilizzavano un apparecchio crittografico chiamato Enigma. Il suo funzionamento era basato su dei rotori e dei cavi intrecciati in maniera ignota. Ogni giorno veniva decisa la disposizione dei rotori e ogni lettera, tramite degli impulsi luminosi veniva convertita con un'altra. Fu violato dall’inglese Alan Turan, considerato anche padre dell’informatica moderna, anche grazie al fatto che quasi tutti i messaggi iniziavano e finivano con le stesse frasi.

5. DES,RSA  
Grazie alla diffusione dei personal computer e soprattutto di Internet abbiamo assistito a un incremento della necessità di messaggi sicuri. Internet infatti è nato come una rete insicura ed era necessario renderla sicura grazie a nuovi algoritmi. È infatti di questo periodo la nascita di molti algoritmi, tra cui DES ed RSA.