Šifra Affine:

Šifra Affine je lineárna substitučná šifra definovaná nad konečným poľom modulo 26. Na rozdiel od Caesarovej šifry rozširuje priestor kľúčov zavedením parametra a, ktorý riadi „sklon“ transformácie. Podmienka je, že a a m (pod m budeme označovať počet písmen abecedy, teda 26) musia mať najväčšieho spoločného deliteľa = 1. Keby táto podmienka nebola splnená, tak by šifra nebola bijektívna, teda by sme mohli dostať dva a viac rôznych textov po rozšifrovaní jedného šifrovaného textu.

Caezarova šifra:

Caezarova šifra je jednou z najjednoduchších substitučných šifier. Jej základná myšlienka spočíva v tom, že každé písmeno otvoreného textu sa nahradí písmenom o určitý počet pozícií posunutým v abecede. História tejto šifry siaha až do starovekého Ríma, kde ju pravdepodobne používal Julius Caesar vo vojenskej komunikácii.

Bezpečnosť tejto šifry je veľmi nízka, keďže existuje len 26 možných kľúčov. Útočník môže šifru prelomiť hrubou silou alebo frekvenčnou analýzou.

Vernamova šifra:

Vernamovu šifru navrhol Gilbert Vernam v roku 1917.Používa bitovú operáciu XOR medzi otvoreným textom a náhodným kľúčom rovnakej dĺžky.Neskôr maďarský matematik J. Mauborgne dokázal, že ak je kľúč:

-úplne náhodný,
-rovnako dlhý ako správa,
-použitý iba raz,
tak vytvára teoreticky nerozbitnú šifru

Vigenèrova šifra:

Vigenèrova šifra je polyalfabetická substitučná šifra, ktorá bola dlho považovaná za nerozbitnú. Používa kľúčové slovo, ktoré určuje sériu posunov v abecede. Tento prístup maskuje frekvenčné vlastnosti jazyka a robí šifru odolnejšou proti jednoduchým útokom. Jednotlive znaky otvoreného textu sa následne posúvajú o k, kde k je znak s indexom i v kľúčovom slove, kde i je získaný ako (pozícia znaku v otvorenom texte % dĺžka kľúčového slova). Po posunutí znaku o k ešte samozrejme musíme spraviť % 26 aby sme dostali korektný znak abecedy.