Symmetric Key Systems:
Csak 1 kulcs létezik. Ezzel lehet az üzenetet/szövege kódolni és dekódolni is. Működése lehetséges, de nagy a rizikó faktor, ezért nem igazán használják módosítások nélkül ezt a módszert.

Assymmetric Key Systems:
Két kulcsos rendszer. Egy publikus és egy privát kulcsot használ.
Publikus kulcs – mindenki számára elérhető
Privát kulcs – csak a 'fogadó fél' által ismert kulcs
Az üzenetet a publikus kulccsal enkriptálják és csak a hozzá illő privát kulccsal lehet dekódolni.

Transparent Database Encryption (TDE):
File szintű titkosítást tesz lehetővé.
Data at rest – olyan adat, amivel a számítógép éppen 'nem foglalkozik' (pl egy szöveges dokumentum)
Data at use – (pl ha az előbb említett szöveges dokumentumot megnyitjuk és szerkeszteni kezdjük)
Olyan adatokat titkosít, amik 'Data at rest' státuszúak, hard drive-ra és folytonosan backup-ként is.
Általában teljes adatbázist titkosít.

Column-Level Encryption
Adatbázisok táblákból állnak, táblák pedig sorokból és oszlopokból. Amíg a TDE általában teljes adatbázist titkosít, addig ez a módszer csak bizonyos oszlopokat, így sokkal rugalmasabbá téve a titkosítási folyamatot, hiszen különböző oszlopok kódolására így használhatóak különböző kulcsok. Negatívuma a nagyobb időigényesség, hiszen az oszlopok külön kulcsokkal vannak enkriptálva, így az adatbázisba való bevitel, keresés, lekérdezés is lassul.

Field-Level Encryption:
Ezzel a módszerrel a szenzitívnek talált információk könnyedén enkriptálhatóak, mező szinten kódolja az adatot, nem oszlop sem teljes adatbázis szinten. Különböző kulcsok használata különböző mezőkre ebben az esetben hatékonyabban kivitelezhető.

Application-Level Encryption:
Mielőtt az adatbázisba bekerülnének az információk, előtte kódolódnak, így már kódolva kerülnek be. Az enkriptálási folyamatot az a program végzi, ami a titkosítandó adattal foglalkozik.

Data Encryption Standard (DES):
Szimmetrikus kulcsos algoritmus. 56 bit kulcs hossz.
Egy meghatározott string típusú szöveget (data block) vesz alapul, majd hosszas bonyolult műveletek elvégzése után egy megegyező méretű titkosított szöveget ad eredmény képpen.
Kulcs egyébként 64 bit hosszú, de abból 8 bit csak az egyezés megvizsgálása érdekében létezik, ezért számolják csak 56 bit hosszúnak.

Triple DES:
A DES algoritmus háromszoros ismétlődése minden egyes data block-on, így a kód feltörése, kulcsok megtalálása, stb.. sokkal időigényesebb és bonyolultabb feladat.

Advances Encryption Standard (AES):

Egy blokk méret 128 bit. Kulcs lehetséges hosszai: 128, 192, 256 bit.

Több fázisból áll, byte-ok eltolása, összekeverése, kulccsal való xor-zása. Bonyolult algoritmus, ezért használják nagyon sok helyen (Apple, Google, Amerikai kormány).

Kulcs mérete határozza meg, hogy hányszor fog az algoritmus végbemenni az adott blokkon (128 – 10x, 192 – 12x, 256 – 14x).

Hashing:

Egyoldalú titkosítási módszer. Eredeti adat visszakapására a hash-elés után nincs lehetőség, ezért használják jelszavak, felhasználónevek, olyan adatok tárolására, aminek csak egyezését kell a későbbiekben vizsgálni és nem kell visszaadni az értékét.