7- 40 kişinin olduğu bir sınıfta herkesin yaşının farklı olma ihtimali 1/40! dir.

8- 1058 ya da 7988

10 – Dizi şifreleme anahtar değiştirmeden kayan anahtar her seferinde farklı initialization vector (IV ) yani başlangıç vektörü kullanılarak sağlanır. IV değeri değiştiğinden her seferinde farklı kayan anahtar oluşur.

11 – Gerçek dünya uyguşlamalrını blok cipher genelde stream cipher dan daha güvenli olarak görülebilir; fakat düzgün implement edilmiş bir stream cipher algoritması blok cipher algoritmalarıyla eşit derece de güvenlik özellikleri sağlayan permutasyon sayısını üretebilir. Performans açısından bakarsak blok cipher key anahtarı oldukça büyüktür ve bu da işlem yapmak için daha fazla kaynak ister ve bu oran stream cipher a göre fazladır diyebilirz. Yani bu bakımdan düşünürsek stream cipher algoritmaları daha hızlı düşünülebilir; fakat kullanılan platforma göre bu farklılık gösterebilir. Yani tercih edildiklere platforma göre performans kıyaslamaları değişebilir.

12 – Bilindiği gibi blok şifreleme de oluşacak permutasyon sayısını artırmak için çevrimler (roundlar) kullanılır. Her çevrimde kullanılacak anahtarı üretmek(belirlemek) için çevrim şeması kullanılır.

13- Herhangi bir metne bir blok şifreleme algoritması uygularsak ve her zaman aynı key i ve aynı IV yi kullanırsak sonuç hep aynı olur. Yani hep aynı şifreli metin elde edilir. Böyle bir durumu ortadan kaldırmak başka deyişle permutasyon sayısını artırmak için blok şifreleminin modları olan CBC, CFB, OFB kullanılır.

CBC de her rounda oluşacak şifreli blok bir önceki blokun değerine bağlıdır, ismini de zaten buradan alır. Bu da demek oluyor ki bu şifreleme modunda paralelleşme mümkün değildir ve algoritmayı çözmek için her zaman permutasyonun tersine ihtiyaç vardır. Herhangi bir hata durumunda bitler iki blok kadar kayar.

CFM modunda şifrelenen bir önceki blok alınır ve plaintext le XOR işlemi yapılarak bir sonraki şifreli blok bulunur. Bu modda paralleşme vardır ve permutasyonun tersine ihtiyaç yoktur. Yani direk şifreli metin kullanılarak decipher işlemi yapılabilir. Herhangi bir hata durumunda bitler hata birkaç blok kadar yayılabilir.

OFB modu çalışma açısından CFB moduna benzer. CFB den farkı ise farklı boyutlardaki blokların şifrelenmesine izin verir. Bu modda paralelleşme yoktur ve permutasyonun terine ihtiyaç duyulmaz. Yani direk şifreli metin kullanılarak decipher işlemi yapılabilir. Herhangi bir hata durumunda bloklarda hatalı bit yayılımı görülmez.