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.