# İlk Günki Quiz Soruları ve Cevapları

Kriptoloji dersinin ilk gününde yapılan quiz soruları ve cevapları

## Tüm Sorular

- `3^-1 (mod 5) = ?`, `3^-1 (mod 6) = ?`
- Cryptolocker ve Bad rabbit nedir?
- Blockchain nedir, neden kullanılır?
- RSA ve AES arasında temel fark nedir?
- Kırılamayan sistem olabilir mi?

## Mod Sorularının Cevapları

Bir sayıyı tersi ile işleme soktuğumuzda birim elemanı vermesi gerekmektedir.

`3^-1 (mod 5) = ?`

- `-1` ise çarpma işlemine göre tersi demektir
- Mod işleminde çarpma işleminin birim elemanı `1` dir
- 3 * [0, 1, 2, 3, 4, 5] (bunlardan her biri) = 1 olmalıdır
- Cevap `2`'dir (3 * 2 = 6 = 1 mod5)

`3^-1 (mod 6) = ?`

Yukarıdaki işlemlerin aynısı denendiği zaman `1` değerini veren bir çarpım bulunmadığından cevap **boş küme**'dir

- 3 * [0, 1, 2, 3, 4, 5] != 1 (eşit değildir)

## Cryptolocker ve Bad rabbit nedir

Temel olarak kullanıcının verilerini şifreleyerek, şifreyi açma karşılığında onlardan para isteme işlemleridir

## Blockchain nedir, neden kullanılır

Blockchain'in temel kullanılma amacı güvenliktir.

- Veriler zincir yapısı ile her bilgisayarda saklanır
- Zincirdeki değişikliğin kabul edilebilmesi için %51 oranında kabul görmesi gerekir
- Zincir bağlantıları sha256 gibi şifreleme yöntemleri ile tek yönlü olarak şifrelenir

## RSA ve AES arasında temel fark nedir

RSA, asimetrik iken AES simetrik bir yaklaşım güder.

## Kırılamayan sistem olabilir mi

Kırılamayan bir sistem tabiki de olamaz 😉

- Şifreleme işlemlerinde güvenliğin ölçütü kırılabilirlik değildir
- Ölçüt ne kadar sürede kıralabileceğidir
- Yani kırılması için çok fazla vakit gerektiren sistemler, daha güvenli olarak ele alınır