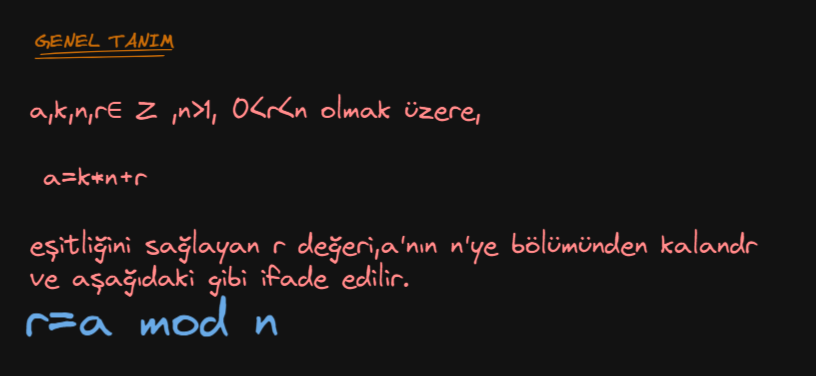
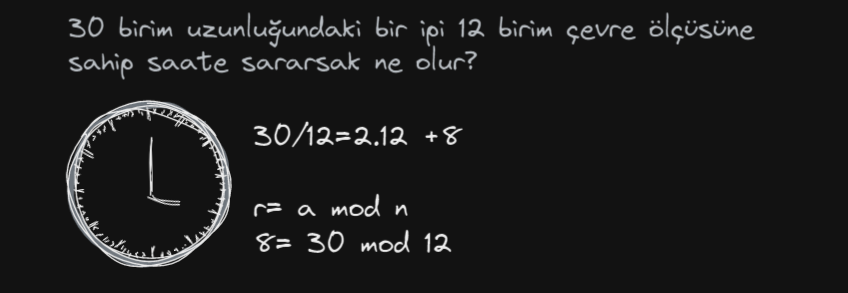
****

**Modüler Aritmetik**

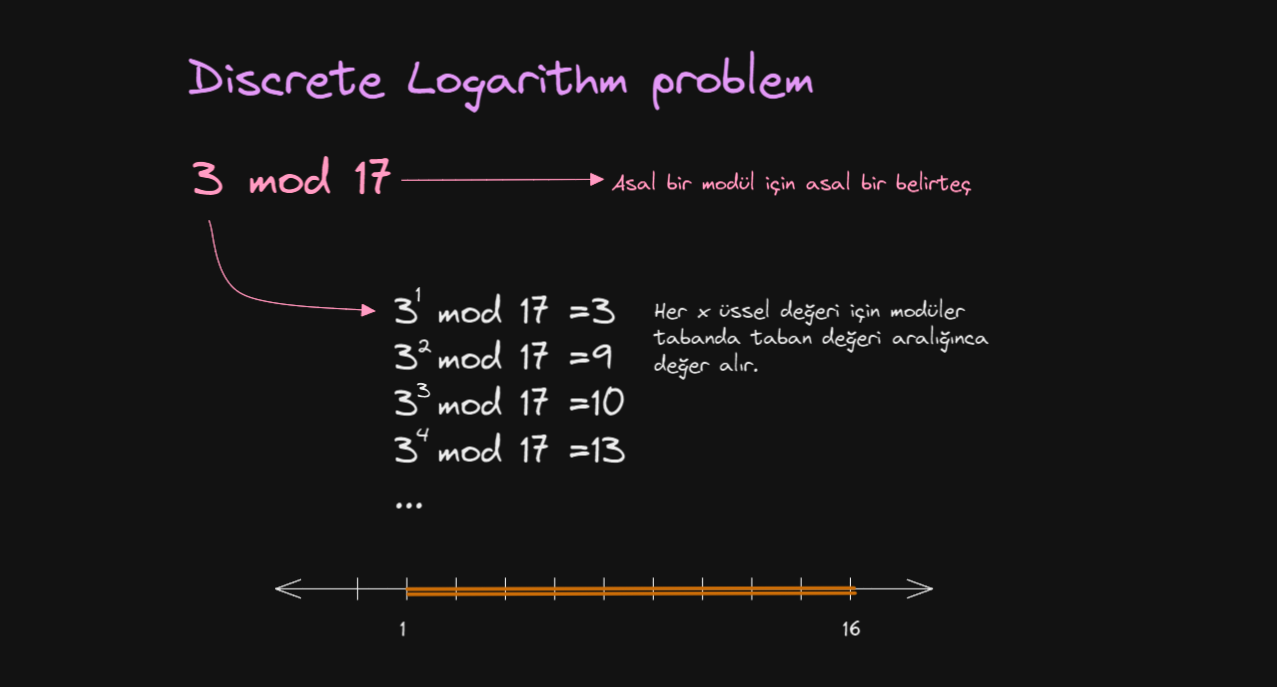
Çift yönlü bir işlem olmasına rağmen bir yönden çok kolay şifrelenip diğer yönden çok zor deşifre edilen matematiksel işlemlerdir.Bu işlem “saat aritmetiği” olarak da adlandırılan modüler aritmetik işlemidir.



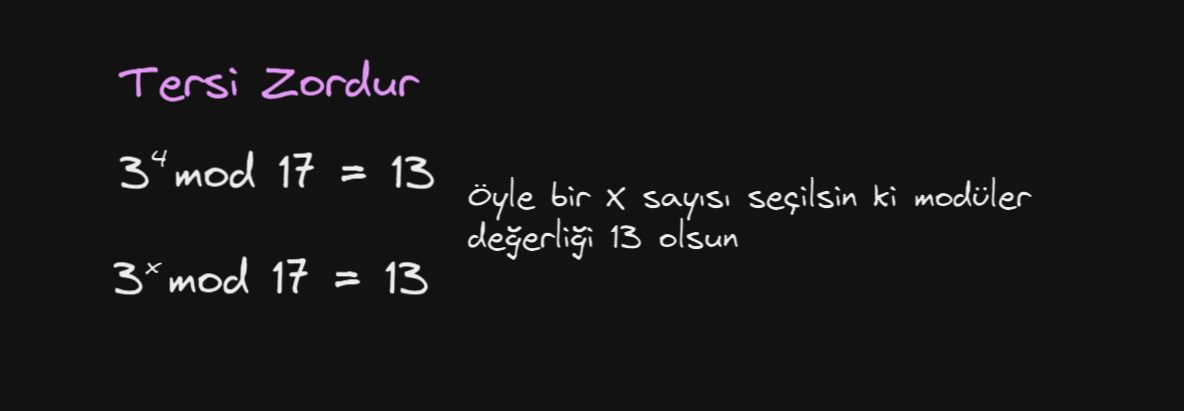
30 birim uzunluğundaki ipi, çevresi 12 birim olan bir saatin etrafına doladığımızı farz edelim.



**Discrete Logarithm problem**

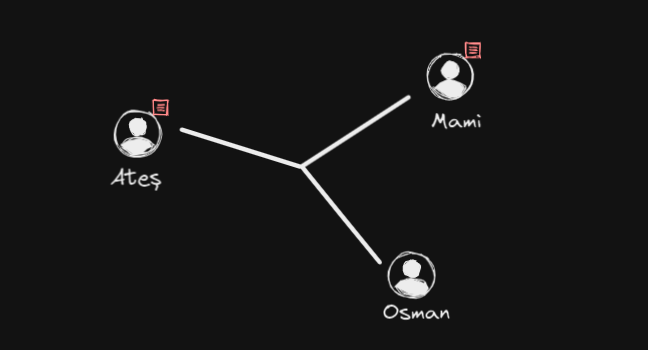
Modül olarak asal bir sayı buluyoruz. Örneğin bu sayı 17 olsun. Sonra bu modül içerisinde bulunan bir asal sayı seçiyoruz. Örneğin bu sayı 3 olsun. Çözüm aralığına bakıldığında değer hep 0 ile modüler değerin arasındadır

Bunun tersini yapmak zordur. Deneme yanılma yolu ile küçük değerlikli sayılar için bu değeri bulmak kolay olabilirir. Fakat yüzlerce basamaklı bir asal sayı için bu değeri bulmak pratikte imkansız sayılır. Dünya üzerinde bulunan bilgisayarlar ve bilgisayar türevi işlemcisi olan cihazlarda bunları yapmak çok zordur.

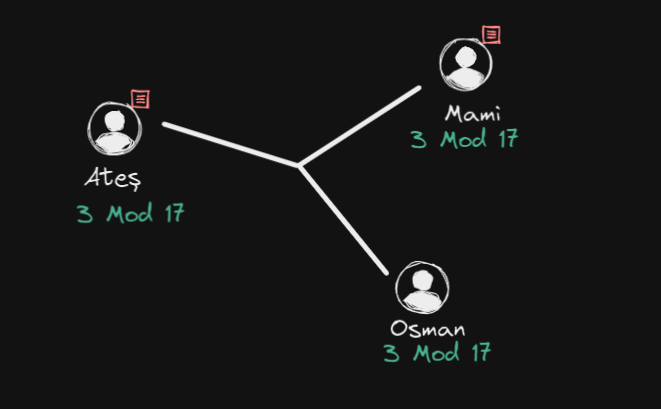


Dipnot: Şifreleme algoritmalarında önemli olan kırılıp kırılmaması değil, ne kadar süre kırılmadan durabileceğidir.

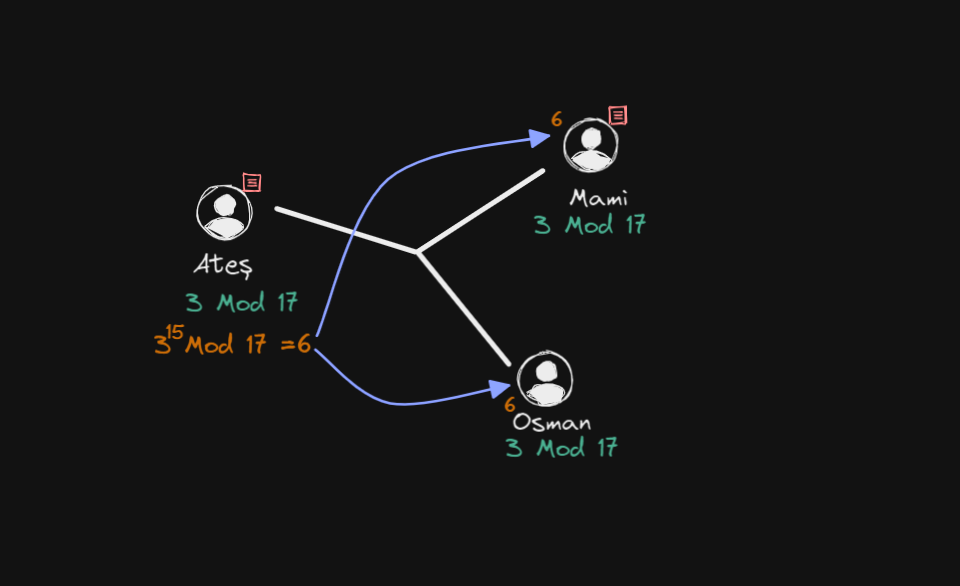
**Diffie-Helman Key Exchange**

****

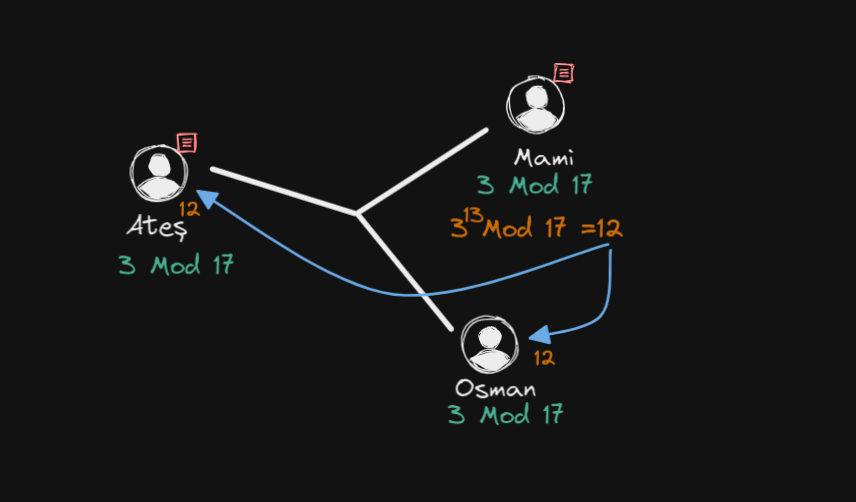
Ateş ve Mami iletişim kurmak istiyor ve bunun için ortak mod ve anahtar belirliyorlar. Örneğin 3 mod 17



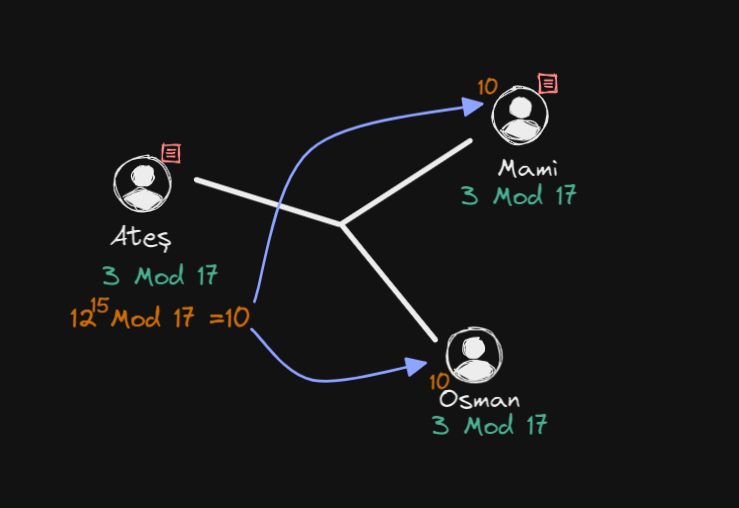
Ateş kafasından bir sayı belirleyerek bunu mod işleminin üssel değerine sokuyor . Örneğin 15. Bu işlem sonucu ortaya çıkan 6 sayısını herkese açık bir şekilde Mami’ye paylaşıyor.

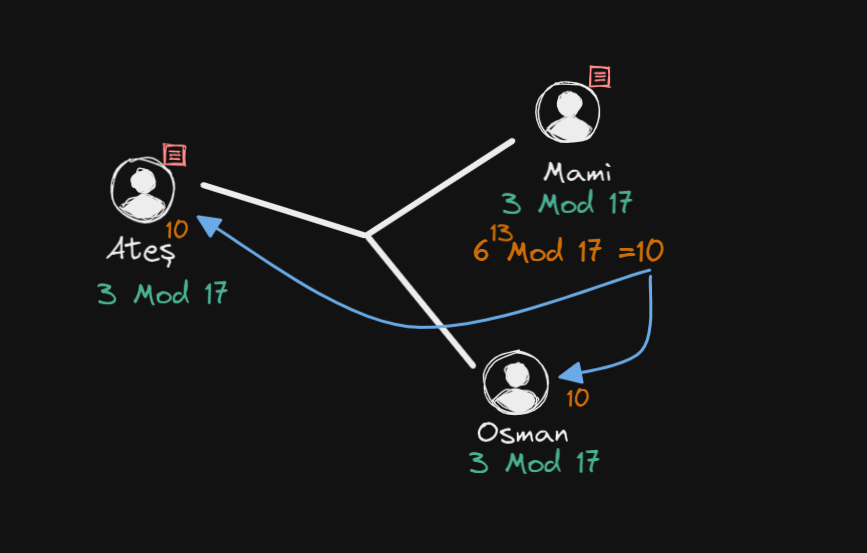


Sonra Mami de aynı şekilde kendi sayısını belirleyip moda sokuyor. Örneğin 13. Bu işlem sonucu ortaya çıkan 12 değerini herkese açık bir şekilde Ateş’e paylaşıyor.



Ateş Mami’nin herkese açık gönderdiği sonucu alıp üssü olarak kendi özel sayısını koyarak tekrardan işleme sokuyor.

Mami de Ateş’in gönderdiği sonucu taban olarak alıp üsse kendi sayısını koyuyor.



Sonuçlar aynı çıkıyor. Bu sayede karşılıklı olarak anlaşabiliyorlar. Bu basit sistemde kendine gelen anlamsız 6 ve 12 sayısını anlamaya çalışan Osman hiçbir şey anlayamıyor.

Bu yöntem sözde rastgele üretilmiş sayı dizileri arasında gerçekleşirse hiç tanışmayan iki kişi arasında da mesajlaşma için kullanılabilir.