Şifreleme

Sır Bölüştürmek

Sonat Süer / sonatsuer@gmail.com*

1. Temel Problem

Diyelim ki elimizde 2 kişiye ait değerli bir nesne var ve bu nesneyi bir kasanın içine koyduk. Nesnenin sahipleri kasanın şifresini bilmek istiyor ama küçük bir sorun var: birbirlerine güvenmiyorlar. Her iki taraf da kendisi kasanın başında değilken diğerinin gelip kasadaki nesneyi çalmasından korkuyor. Yani öyle bir yol bulmalıyız ki kasa sadece her iki taraf da kasanın başındayken açılabilsin.

İlk akla gelen şifreyi ikiye ayırmak. Diyelim ki kasanın şifresi dört haneli bir

$$a_1a_2a_3a_4$$

sayısı. Bir tarafa a_1a_2 sayısını verip bunun ilk 2 hane olduğunu, diğer tarafa da a_3a_4 sayısını verip bunun son 2 hane olduğunu söylediğimizi düşünelim. Bu durumda iki taraf da şifrenin tamamını bilmiyor, yani tek başına kasayı açamıyor ama bir araya geldiklerinde şifrenin tamamını oluşturabiliyorlar. Problemi çözdük. Ya da çözdük mü? Yukarıda "hiç bir taraf tek başına kasayı açamıyor" dedik ama biraz dikkat edince doğru cümlenin "iki taraf da büyük ihtimalle ilk denemede kasayı açamıyor" olması gerektiği anlaşılıyor. Açıklayalım. Diyelim ki a_1a_2'yi biliyoruz ama a_3a_4'ten haberimiz yok. Bu durumda teker teker

a_1a_200, a_1a_201, a_1a_202, a_1a_203, a_1a_204, ...

sayılarını deneyebiliriz ve en kötü ihtimalle 100 deneme sonra kasayı açarız. Şifre hakkında hiçbir şey bilmeseydik en kötü ihtimalle 10.000 deneme yapmamız gerekecekti. Yani, her ne kadar şifrenin tamamını bilmesek de, şifrenin bir kısmını bilmek kasayı açmamızı ciddi şekilde kolaylaştırıyor. Elbette bunun olmasını istemiyoruz.

Yapmamız gereken, şifreyi, hiçbir parçanın tek başına şifrenin tamamı hakkında bilgi vermeyeceği bir şekilde parçalara ayırmak. Bunu yapmak da zor değil. Önce 4 haneli rastgele bir $r_1r_2r_3r_4$ sayısı seçip taraflardan birine bu sayıyı verelim. Diğer tarafa da haneleri $i = 1, 2, 3, 4$ için

$$b_i = a_i - r_i \pmod{10}$$

kuralıyla tanımlanan $b_1b_2b_3b_4$ sayısını verelim. Bu iki parçadan şifreyi, yani $a_1a_2a_3a_4$ sayısını oluşturmak kolay:

$$a_i = b_i + r_i \pmod{10},\ i = 1, 2, 3, 4.$$

Üstelik $r_1r_2r_3r_4$ rastgele olduğu için hiçbir parça şifreyle ilgili ipucu vermiyor.

Eğer 2 yerine N kişi varsa $N - 1$ tane 4 haneli rastgele sayı kullanarak çözümü genelleştirmek de mümkün. Bu sayıları $j = 1, 2, ..., N - 1$ için

$$r_1^j r_2^j r_3^j r_4^j$$

ile gösterelim. Tek yapmamız gereken $N - 1$ kişiye bu rastgele sayıları vermek, N'inci kişiye de $i = 1, 2, 3, 4$ için

$$b_i = a_i - (r_i^1 + \cdots + r_i^{N-1}) \pmod{10}$$

kuralıyla tanımlanan $b_1b_2b_3b_4$ sayısını vermek. Tabii şifrenin kaç haneli olduğunun bir önemi yok. Hatta şifrenin 10'luk tabanda olmasının da bir önemi yok.

2. Shamir Sır Bölüştürme Yöntemi

Şimdi problemi biraz değiştirelim. Diyelim ki elimizde 100 kişiye ait değerli bir nesne var ve bu nesneyi gene bir kasanın içine koyduk. Ama bu sefer nesnenin sahipleri teker teker birbirlerine güvenmeseler de salt çoğunluğun kararına güveniyorlar. Yani 100 kişiden en az 51 kişinin, kasayı açmak konusunda fikir birliğine vardıklarında, geri kalanlara ihtiyaç duymadan kasayı açabildiği bir yöntem bulmalıyız.

İlk adım olarak yukarıdaki çözümü bu duruma uyarlamayı deneyelim. Önce 100 kişilik grubun her 51 kişilik altkümesine bir numara verelim. Sonra k numaralı altküme için 50 tane rastgele sayı kullanarak yukarıdaki gibi şifreyi 51 parçaya böle-

* İstanbul Bilgi Üniversitesi öğretim üyesi.

lim ve buna k numaralı parçalanış diyelim. Şimdi 100 kişilik grubun herhangi bir üyesine, her k için, eğer k numaralı altkümenin ℓ'inci üyesiyse k-numaralı parçalanışın ℓ numaralı parçasını (k numaralı parçalanışa ait olduğunu belirterek) verelim.

Bu durumda eğer 51 kişilik bir altküme toplanırsa şifreyi tekrar oluşturabilir. Yapmaları gereken ilk önce kaç numaralı altküme olduklarını bulmak. Herkes elindeki her parçanın kaç numaralı parçalanıştan geldiğini bildiğinden bunu yapmak mümkün. Diyelim ki numaralarını k olarak buldular. Ellerinde k numaralı parçalanıştan gelen parçaları kullanarak şifreyi yeniden oluşturabilirler çünkü k numaralı parçalanışın her parçası bu gruptan bir kişinin elinde. Teorik olarak problemi çözdük ama pratikte bu yöntemi uygulamak çok zor çünkü 100 elemanlı bir kümenin astronomik sayıda (yaklaşık 10^{29} tane) 51 elemanlı altkümesi var.

Şimdi probleme Adi Shamir'in[1] getirdiği zarif çözümü vereğiz. Önce problemi genel biçimde ifade edelim. Elimizdeki S doğal sayısıyla ifade edilen sırrı N kişi arasında şu koşulları sağlayacak şekilde bölüştürmek istiyoruz:

1. Eğer M kişi bir araya gelirse S sayısını kolayca hesaplasın,

2. Eğer $M - 1$ ya da daha az kişi bir araya gelirse S sayısını hesaplamak için bir avantajları olmasın.

Önce S ve N'den daha büyük bir p asalı alalım ve $\mathbb{Z}/p\mathbb{Z}$ içinden rastgele $a_1, a_2, \ldots, a_{M-1}$ elemanları seçelim. S sayısının $\mathbb{Z}/p\mathbb{Z}$'deki görüntüsü de a_0 olsun. Şu polinomu tanımlayalım:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{M-1}x^{M-1}.$$

Sırrı bölüştüreceğimiz M kişiden i'incisine $(i, f(i))$ ikilisini verirsek problemi çözmüş oluyoruz. Öncelikle f polinomunun derecesi $M - 1$ ve dolayısıyla M noktada aldığı değerle belirleniyor. Hatta Lagrange interpolasyon formülü bize genel olarak bir cisimde her $i = 0, \ldots, n$ için α_i noktasında β_i değerini alan ve derecesi n olan polinomun

$$\sum_{i=0}^{n}\left(\beta_i \prod_{\substack{0 \le j \le n \\ i \ne j}} \frac{x-\alpha_j}{\alpha_i-\alpha_j}\right)$$

olduğunu söylüyor. Polinomu bulabiliyorsak 0'da aldığı değeri, yani a_0'ı da bulabiliriz. Yani M kişi a_0'ı ve dolayısıyla S'yi bulabiliyor. Ama daha az sayıda kişi a_0 hakkında hiç bilgiye sahip olmuyor çünkü dercesi $M - 1$ olan bir polinomun 0 dışındaki $M - 1$ noktada aldığı değer 0'da alabileceği değeri hiçbir şekilde kısıtlamıyor.

3. Görsel Şifreleme

Son olarak Moni Naor ve Adi Shamir'e ait görsel şifreleme adında başka bir sır bölüştürme yönteminden bahsedeceğiz. Görsel şifrelemenin ilginç yönü bölüştürülen bilginin bir resim olması. Resimlerimizin saydam ya da opak piksellerden oluşan birer matris olduğunu ve cam gibi saydam bir zemin üzerine basıldığını düşüneceğiz. Eğer X bir resimse X_{ij} ile matrisin (i, j) indeksli girdisini ifade edeceğiz. Bir resmi gene resim olan parçalara ayıracağız ve orjinal resmi yeniden kurmak, parçaları üstüste oturtmaktan ibaret olacak.

İşimizi kolaylaştırmak için bir resmi 2 kişi arasında paylaştırma problemiyle ilgileneceğiz. İstediğimiz elbette parçaların orjinal resim hakkında hiç bilgi vermemesi.

Önce iki pikseli üstüste oturtunca ne olduğuna bakalım. Eğer o opak bir pikseli, s saydam bir pikseli ve + üstüste oturtma işlemini ifade ediyorsa elimizde şöyle bir toplam tablosu var:

+	s	o
s	s	o
o	o	o

Yani iki pikselin saydam bir piksel vermesi için gerekli ve yeterli koşul ikisinin de saydam olması.

Diyelim ki R resmini A ve B diye iki parçaya ayırdık. Yani A ve B'yi üstüste koyunca R'yi elde ediyoruz. Pikseller seviyesinde bu her (i, j) için

$$A_{ij} + B_{ij} = R_{ij}$$

olması demek. Eğer $A_{ij} = s$ olduğunu biliyorsak B_{ij}'nin ne olduğunu bilmeden R_{ij}'nin ne olduğunu anlamak mümkün değil çünkü

$$s + o = o \text{ ve } s + s = s.$$

Diğer yandan $A_{ij} = o$ ise $R_{ij} = o$ olmak zorunda çünkü hem $o + o = o$ hem de $o + s = o$. Yani A hakkındaki bilgimiz bize R hakkında bilgi veriyor. Dediğimiz gibi bunun olmasını istemiyoruz.

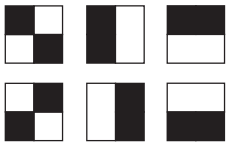
Durumun vehametini göstermesi için aşağıdaki figürde bu yöntemi kullanarak bir resmi sağdaki iki parçaya ayırdık. Opak olan pikseller rastgele $s + o$ ya da $o + s$ olarak parçalanıyorlar ama saydam olanlar için $s + s$ tek seçenek. Solda duran orjinal resim iki parçada da deyim yerindeyse kabak gibi ortada.

1 Adi Shamir, Ron Rivest ve Len Adleman ile birlikte meşhur RSA şifreleme yöntemini bulan matematikçidir.

Bu yöntemin, eğer resmin piksellerini bir kasa şifresinin haneleri gibi görürsek, ilk bölümde verilen yönteme çok benzediğine okurun dikkatini çekelim. Yalnız orada kullanılan + işlemi mod 10'da toplamaydı ve dolayısıyla $x + a = y$ denkleminde x'i bilmeden a'yı bilmek bize y hakkında hiç fikir vermiyordu. Ama ($\{s, o\}$, +) yapısında (ne olduğunu bilenler için, monoidinde) bu doğru değil.

Şimdi Naor ve Shamir'in bu probleme getirdiği çözümü açıklayalım. Fikir saydam pikselleri yarı saydam yarı opak hale getirmek. Ama elimizdeki pikseller ya saydam ya opak olduğundan bunu yapmak için orjinal resimdeki her pikseli 2 × 2'lik bir resimle ifade edeceğiz. Böylece parçalardaki piksel sayısı orjinal resimdeki piksel sayısının 4 katı olacak.

Olası $2^4 = 16$ tane 2 × 2'lik resim var ama biz bunlardan sadece 2 opak ve 2 saydam piksel içeren 6 tanesini kullanacağız. Aşağıdaki figürde bu 6 resim var.



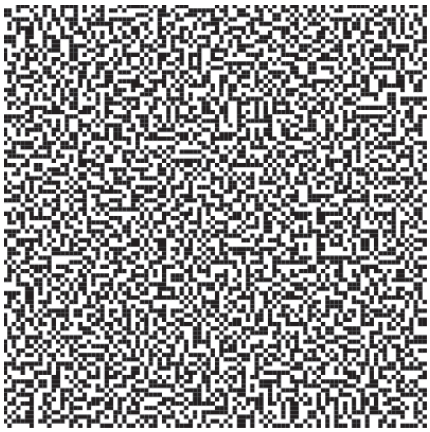
Bu 6 resme süper piksel diyelim. Eğer A bir süper pikselse A'nın tümleyeni A'daki opak piksellerin saydam, saydam piksellerin opak yapılmasıyla elde edilen resim olsun. Bir süper pikselin tümleyeninin de süper piksel olduğu açık. Yukarıdaki figürde birbirinin tümleyeni olan süper pikselleri aynı sütuna yerleştirdik. Ayrıca kolayca görüldüğü üzere bir süper piksel ve tümleyeninin üstüste oturtulmasıyla 4 opak piksel elde ediliyor.

Şimdi iki parçaya ayıracağımız R resmini alalım. İlk parça R'nin sadece ölçülerine bağlı olacak. Önce ölçüleri R'nin ölçülerinin 2 katı olan ve dolayısıyla R'nin 4 katı piksel içeren tamamen saydam bir resim alalım. Bu resmi 2×2'lik kutulara bölelim. Elbette böylece R'nin piksel sayısı kadar kutu elde ederiz. Şimdi her kutunun üstüne rastgele bir süper piksel oturtalım. Bu şekilde elde ettiğimiz resme A diyelim. Bu resim birinci parçamız olacak.

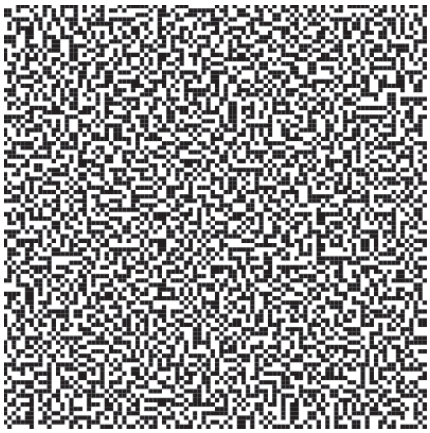
İkinci parçayı kurmak için R'yi kullanacağız. Önce A ile aynı boyda tamamen saydam bir resim alalım ve gene A da olduğu gibi resmi 2×2'lik kutulara bölelim. Her (i, j) için $(2i, 2j)$ indeksli pikseli içeren kutuya R_{ij} pikseline denk gelen kutu diyelim. Şimdi her (i, j) için şunu yapacağız: Eğer R_{ij} saydamsa, R_{ij}'ye denk gelen kutuya A'da R_{ij}'ye denk gelen süper pikselin aynısını, opaksa A'da R_{ij}'ye denk gelen süper pikselin tümleyenini oturtalım. Bu şekilde elde ettiğimiz resme B diyelim. Bu resim de ikinci parçamız olacak.

Eğer A ve B'yi üstüste koyarsak R_{ij}'ye denk gelen kutuda eğer R_{ij} saydamsa bir süper piksel, opaksa 4 opak piksel olacak. Ama süper pikseller iki saydam piksel içerdiğinden göze gri gibi görünecekler. Böylece resmi, beyazları grileştirilmiş bir biçimde de olsa, elde edeceğiz.

En sonda bu yöntemle iki parçaya ayrılmış bir resim örneği verdik. Merak eden okur sayfanın asetata fotokopisini çektirip gizli resmin ne olduğuna bakabilir. ♣



Birinci Parça



İkinci Parça