

**Dönem Projesi - Rapor**

**Projede Kullanılacaklar**

**Proje Başlığı**

Dropbox ile Güvenli Veri Paylaşımı

**Takım Üyeleri**

* **Emre Duman 031990002 (**[**031990002@ogr.uludag.edu.tr**](mailto:031990002@ogr.uludag.edu.tr)**)**

**2.**

**3.**

**Takım No:\_\_14\_\_**

**İçindekiler**

Özet...2

1.Problem Tanımı..2

2.Giriş...3

3. Alternatif Çözüm Araştırmaları...3

3.1. AES Algoritması...3

3.2. Blowfish Algoritması ..4

3.3. XOR Brute Force Algoritması ...4

3.4. Enigma Algoritması ...4

3.5. Atbash Algoritması ....5

3.6. Vigenere Algoritması ..5

3.7. DES Algoritması ....6

3.8. Diffie-Hellman Anahtar Değişim ...6

3.9. RSA (Rivest-Shamir-Adleman) ...7

3.10. (ECC) Elliğtic Curve Cryptoraphy...7

4. Önerilen Çözümün Kısıtlamaları...8

5. Çözüm Yöntemi ...8

Kaynakça ....8

**Özet**

Yaşanabilecek veri hırsızlıkları gibi olayların ciddi kurumsal ve kişisel sıkıntıları bulunmaktadır. Her ne kadar güvenli olduğunu savunan programlar bulunmakta olmasına rağmen kötü düşünceli insanlar programları hackleyerek verilere erişmeye ve hırsızlık yapmaya çalışmaktadır. Bütün programların şifreleri kırılabilir buna bizim yapacağımız program da dahil ancak projemizin ne kadar dinamik ve hackerı ne kadar uğraştıracak komplekslikte olursa erişimi o kadar zorlaştırır ve engeller.

Yaptığımız araştırmalarla bulduğumuz algoritmaların birbirleri arasında karşılaştırılması ve değerlendirilmesi sonucunda verilerimizin kullanıcılar arası gönderilirken kullanılacak şifreleme algoritmasını kendi yazdığım karma bir Brute Force Algoritması yoluyla şifrelenecektir ve bu algoritmada kullanılacak anahtarımız da Diffie-Hellman**[4.1]** algoritması yardımı ile belirlenecektir. Ardından kullanıcılarımız arayüzümüzdeki etkileşimleri kullanarak verilerini istedikleri kişilere üçüncü kişilerin erişse bile anlayamayacağı şekilde şifrelenmiş bir şekilde iletebilmesi hedeflenmektedir.

**1.Problem Tanımı**

Müşterilerin başka bir kişiye göndermek istediği verilerin Dropbox üzerinden gönderilirken Dropbox’ta oluşabilecek sızıntı, hacklenme, Dropbox mühendisinin işini kötüye kullanımı gibi çeşitli olaylar sonucu verilerimizin üçüncü şahıslar tarafından ele geçirilse bile mantıklı bir veri elde edememesini sağlamak istemektedir.

**2.Giriş**

Hackerların çokluğu ve anlamlı verilerin değerliliği bakımından veri hırsızlığı, sızıntılar günümüzde çok yaygın olmakla birlikte milyonlarca dolarlık hırsızlıklar yapılmaktadır.

Anlık olarak, çeşitli hack önleme uygulamaları bulunmaktadır örneğin, İki faktörlü doğrulamalar, virüs tarama uygulamaları, windows defender etc.. Ancak bu uygulamalar ne yazık ki yetersiz kalmaktadır. Bunların yanı sıra şifreleme algoritmaları da bulunmaktadır. Bunlara **[3. Bölüm]** rapor içerisinde değindik.

Bu nedenle, yapacağımız proje kullanacağımız uygulamalardaki üçüncü şahısları bırakın uygulama sahipleri, uygulamanın mühendisleri bile verilerimizi anlamlandıramamasını sağlayacak gereksinimleri araştırdım.

-- Verilerimizi şifrelemek için kullanacağımız şifreleme algoritmalarını araştırdım.

-- Verilerimizi şifreleyeceğimiz anahtarların(key) kullanıcılar arası nasıl iletilebileceğini araştırdım.

-- Dropboxa yapacağımız çeşitli istekleri sağlayan apilerin araştırmasını yaptım.

-- Kullanıcının rahat edebileceği açık arayüz tasarımı nasıl yapabileceğimi araştırdım.

Hedefimiz, olası kötü amaçlı insanların çeşitli kişiler arası yapılan veri alışverişi sırasında kişilerin verilerinin şifrelenip üçüncü şahısların eline geçse bile anlamlı veri ile karşılaşmasını ve bu veriyi anlamlaştırmasını engellemektir.

Bu raporun devamında araştırmalarımızı, edindiğimiz sonuçları, karşılaştığımız problemleri, sıkıntılı süreçleri, riskleri, ve projeyle alakalı yorumlarımızı sizlere aktaracağım.

**3. Alternatif Çözüm Araştırmaları**

**3.1. AES Algoritması**

AES (Advanced Encryption Standard; *Gelişmiş Şifreleme Standardı*), elektronik verinin şifrelenmesi için sunulan bir standarttır. Amerikan hükûmeti tarafından kabul edilen AES, uluslararası alanda da defacto [şifreleme](https://tr.wikipedia.org/w/index.php?title=%C5%9Eifreleme&action=edit&redlink=1) (kripto) standardı olarak kullanılmaktadır. [DES](https://tr.wikipedia.org/wiki/DES)'in (Data Encryption Standard - Veri Şifreleme Standardı) yerini almıştır. AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik-anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.

AES, ABD Ulusal Standart ve Teknoloji Enstitüsü ([NIST](https://tr.wikipedia.org/wiki/NIST)) tarafından 26 Kasım 2001 tarihinde US FIPS PUB 197 kodlu dokümanla duyurulmuştur. Standartlaştırma 5 yıl süren bir zaman zarfında tamamlanmıştır. Bu süreçte AES adayı olarak 15 tasarım sunulmuş, tasarımlar güvenlik ve performans açısından değerlendirildikten sonra en uygun tasarım standart şifreleme algoritması olarak seçilmiştir. Federal hükûmetin Ticaret Müsteşarı'nın onayının ardından 26 Mayıs 2002 tarihinde resmî olarak etkin hâle gelmiştir. Hâlihazırda birçok şifreleme paketinde yer alan algoritma Amerikan Ulusal Güvenlik Teşkilatı ([NSA](https://tr.wikipedia.org/wiki/NSA) - National Security Agency) tarafından çok gizli bilginin şifrelenmesinde kullanımı onaylanan kamuya açık ilk şifreleme algoritmasıdır.

AES ile standartlaştırılan algoritma, esas olarak [Vincent Rijmen](https://tr.wikipedia.org/w/index.php?title=Vincent_Rijmen&action=edit&redlink=1) ve [Joan Daemen](https://tr.wikipedia.org/w/index.php?title=Joan_Daemen&action=edit&redlink=1) tarafından geliştirilen [Rijndael](https://tr.wikipedia.org/w/index.php?title=Rijndael&action=edit&redlink=1) algoritmasında bazı değişiklikler yapılarak oluşturulmuştur. Rijndael, geliştiricilerin isimleri kullanılarak elde edilen bir isimdir: RIJmen aNd DAEmen.

AES hakkında önemli bir nokta AES'in şifreleme standardının ismi olmasıdır. Ancak pratik kullanımda AES, standartta belirtilen şifreleme algoritmasının yerine geçecek şekilde kullanılmaktadır. Kolaylık ve literatürle uyumlu olması açısından bu dokümanda da standartta belirtilen algoritma AES olarak anılacaktır.**[1]**

**3.2. Blowfish Algoritması**

Blowfish, [Bruce Schneier](https://tr.wikipedia.org/w/index.php?title=Bruce_Schneier&action=edit&redlink=1) tarafından 1993 yılında tasarlanmış, çok sayıda şifreleyici ve [şifreleme](https://tr.wikipedia.org/w/index.php?title=%C5%9Eifreleme&action=edit&redlink=1) ürününe dahil olan; anahtarlanmış, [simetrik](https://tr.wikipedia.org/wiki/Simetrik_%C5%9Fifreleme) bir [Block Cipher](https://tr.wikipedia.org/w/index.php?title=Block_Cipher&action=edit&redlink=1) (öbek şifreleyici)dir. Blowfish ile ilgili olarak şu ana kadar etkin bir şifre çözme analizi var olmasa da, artık [AES](https://tr.wikipedia.org/wiki/AES) ya da [Twofish](https://tr.wikipedia.org/wiki/Twofish) gibi daha büyük ebatlı öbek şifreleyicilerine daha fazla önem verilmektedir.

Schneier; Blowfish'i bir genel kullanım algoritması olarak, eskiyen [DES](https://tr.wikipedia.org/wiki/DES)'ın yerini alması için ve diğer algoritmalarla yaşanan sorunlara çözüm olarak tasarlamıştır. O zamanlarda, birçok diğer tasarım lisanslı, patentle korunmakta ya da devlet sırrı olarak saklanmaktaydı.**[2]**

Bruce Schneier, bunu şu şekilde ortaya koymaktadır : *“Blowfish, patentsizdir ve tüm ülkelerde bu şekilde yer alacaktır. Algoritma genel kamusal alanda bulunmakta olup, herkes tarafından özgürce kullanılabilir.”*

Piyasada kullanılan en hızlı blok şifreleyicilerdendir. Karmaşık anahtar çizelgesi kullanarak kırılmasını zorlaştırır. Blowfish, 23'den 448 bite kadar anahtar uzunluklarına sahiptir. Çalışabilmesi için 4 kilobyte RAM’den daha fazla belleğe ihtiyaç duyarlar. Bu nedenle en küçük gömülü sistemlerde kullanılamazlar.**[3]**

**3.3. XOR Brute Force Algoritması**

XOR Brute Force Algoritması elde edilen karakterlerin binary değerlerine dönüştürülüp XOR kapısı yardımı ile şifrelenmesidir.

**3.4. Enigma Algoritması**

Enigma; [II. Dünya Savaşı](https://tr.wikipedia.org/wiki/II._D%C3%BCnya_Sava%C5%9F%C4%B1) sırasında [Nazi Almanyası](https://tr.wikipedia.org/wiki/Nazi_Almanyas%C4%B1) tarafından gizli mesajların [şifrelenmesi](https://tr.wikipedia.org/wiki/%C5%9Eifre) ve tekrar çözülmesi amacı ile kullanılan bir [şifre](https://tr.wiktionary.org/wiki/%C5%9Fifre) [makinesi](https://tr.wikipedia.org/wiki/Makine). Daha açık bir ifade ile [Rotor makineleri](https://tr.wikipedia.org/wiki/Rotor_makinesi) ailesi ile ilişkili bir [Elektro-Mekanik](https://tr.wikipedia.org/wiki/Elektro-Mekanik) aygıttı ve birçok değişik türü vardı.

Enigma makinesi, ticari olarak 1920 li yılların başında kullanılmaya başlandı. Birçok ülkede [Ordu](https://tr.wikipedia.org/wiki/Ordu_(askeriye)) ve [Devlet](https://tr.wikipedia.org/wiki/Devlet) kurumları için özel modeller üretildi. Bunların en ünlüleri [II. Dünya Savaşı](https://tr.wikipedia.org/wiki/II._D%C3%BCnya_Sava%C5%9F%C4%B1) öncesinde ve savaş sırasında [Nazi Almanyası](https://tr.wikipedia.org/wiki/Nazi_Almanyas%C4%B1)'nda kullanılan modellerdi. [Alman](https://tr.wikipedia.org/wiki/Almanlar) ordu modeli olan [Wehrmacht](https://tr.wikipedia.org/wiki/Wehrmacht) [Enigma](https://tr.wikipedia.org/wiki/Enigma), en çok konuşulan modeldi.

Bu makine kötü bir üne sahip oldu çünkü [Müttefik](https://tr.wikipedia.org/wiki/M%C3%BCttefik) şifreciler ([Polonya](https://tr.wikipedia.org/wiki/Polonya) şifre bürosu, [Birleşik Krallık](https://tr.wikipedia.org/wiki/Birle%C5%9Fik_Krall%C4%B1k) - [Bletchley Park](https://tr.wikipedia.org/wiki/Bletchley_Park) vb.) tarafından geniş mesajları çözümlendi. [Şifre çözücülerin](https://tr.wikipedia.org/w/index.php?title=%C5%9Eifre_%C3%A7%C3%B6z%C3%BCc%C3%BCler&action=edit&redlink=1) [Müttefiklerin](https://tr.wikipedia.org/wiki/M%C3%BCttefikler) savaşı kazanmalarına büyük yardımları olmuştu. Bazı tarihçiler, Alman [Enigma](https://tr.wikipedia.org/wiki/Enigma) kod sisteminin [deşifre](https://tr.wikipedia.org/wiki/De%C5%9Fifre) olması sayesinde [Avrupa](https://tr.wikipedia.org/wiki/Avrupa)'da savaşın iki yıl daha önce bittiğini ileri sürmektedirler.

Enigma şifresinin bazı zayıf yanları olmakla birlikte, aslında diğer [faktörler](https://tr.wikipedia.org/wiki/Fakt%C3%B6r) olan [operatör](https://tr.wikipedia.org/wiki/Operat%C3%B6r) hataları, [prosedür](https://tr.wikipedia.org/w/index.php?title=Prosed%C3%BCr&action=edit&redlink=1) açıkları ve nadir olarak ele geçen [kod](https://tr.wikipedia.org/wiki/Kod) kitapları sayesinde çözümlenebildi.

[II. Dünya Savaşında](https://tr.wikipedia.org/wiki/II._D%C3%BCnya_Sava%C5%9F%C4%B1) [Bletchley Park](https://tr.wikipedia.org/wiki/Bletchley_Park) - [Birleşik Krallık](https://tr.wikipedia.org/wiki/Birle%C5%9Fik_Krall%C4%B1k)'ta üslenen [Amerikalı](https://tr.wikipedia.org/wiki/Amerikal%C4%B1lar) ve [İngiliz](https://tr.wikipedia.org/wiki/%C4%B0ngilizler) şifre çözücüler, o zamanın en yetenekli ve en değerli [bilim insanı](https://tr.wikipedia.org/wiki/Bilim_insan%C4%B1), [matematikçi](https://tr.wikipedia.org/wiki/Matematik%C3%A7i) ve [mühendis](https://tr.wikipedia.org/wiki/M%C3%BChendis) lerinden oluşmaktaydı.Bunlardan bazıları, daha sonra [Bilgisayar biliminin](https://tr.wikipedia.org/wiki/Bilgisayar_bilimi) kurucularından sayılacak [Alan Matthison](https://tr.wikipedia.org/wiki/Alan_Turing) [Turing](https://tr.wikipedia.org/wiki/Turing) ve dünyanın ilk dijital ve programlanabilir bilgisayarı olan [Colossus](https://tr.wikipedia.org/wiki/Colossus_bilgisayar%C4%B1)'u yapan [Thomas Harold Flowers](https://tr.wikipedia.org/wiki/Thomas_Flowers)'dır. Birçok [Colossus bilgisayarı](https://tr.wikipedia.org/wiki/Colossus_bilgisayar%C4%B1), II. Dünya Savaşı sırasında [Alman](https://tr.wikipedia.org/wiki/Almanlar) [Lorenz SZ40/42](https://tr.wikipedia.org/wiki/Lorenz_SZ40/42) şifre sisteminin çözülmesi işleminde olasılık hesaplayıcı olarak kullanılmıştır.

[II. Dünya Savaşı](https://tr.wikipedia.org/wiki/II._D%C3%BCnya_Sava%C5%9F%C4%B1) ve [stratejik](https://tr.wikipedia.org/wiki/Stratejik) planların aktarılmasında kullanılan şifre sistemleri ve bunların çözülmesinde kullanılan algoritmalar, buluşlar, şifre çözücü makineler bir anlamda bilgisayar biliminin doğmasına neden olmuştur diyebiliriz.**[4]**

**3.5. Atbash Algoritması**

Atbash, ([İbranice](https://tr.wikipedia.org/wiki/%C4%B0branice): אתבש), bir metni şifrelemek veya şifresini çözmek için [İbrani alfabesine](https://tr.wikipedia.org/wiki/%C4%B0brani_alfabesi) temelli basit bir yöntemdir. Orijinal [Kabalacı](https://tr.wikipedia.org/wiki/Kabalac%C4%B1l%C4%B1k) yöntem, dinî metinlerde saklı olduğuna inanılan bir anlamın çözülebilmesi amacını taşıyordu.

Atbash adı, İbranice yazı sisteminin (A-T-B-Sh) ilk ve son iki harfinden türetilmiştir ve aynı zamanda ilk harfin (Aleph) son harfle ([Taw](https://tr.wikipedia.org/wiki/Tav)), ikinci harfin (Taw) değiştirildiği prosedürü gösterir. ([Beth](https://tr.wikipedia.org/wiki/Beth)) harfi, sondan bir önceki harf ([Şin](https://tr.wikipedia.org/wiki/%C5%9Ein_(%C4%B0brani_alfabesi))) vb. ile değiştirilir.

Atbash değeri, karşılık geldiği harfin [sayısal değerini](https://tr.wikipedia.org/wiki/Ebced_hesab%C4%B1) ifade eder. Çünkü İbranice her harfin bir [ebced](https://tr.wikipedia.org/wiki/Ebced_rakamlar%C4%B1) değeri vardır. Örneğin; Alef (1) ve Tav (400) değerine sahipken, *Atbash* kelimesinin değeri 400+1'dir. **[5]**

**3.6. Vigenere Algoritması**

Vigenère şifrelemesi, [alfabetik](https://tr.wikipedia.org/wiki/Alfabe) bir şifreleme metni kullanarak bir dizi farklı [Sezar şifrelemesine](https://tr.wikipedia.org/wiki/Sezar_%C5%9Fifrelemesi) dayalı harfleri kullanan bir şifreleme yöntemidir. Bu bir çeşit [poli alfabetik ikame](https://tr.wikipedia.org/wiki/Vigenere_tablosu) tablosudur.

Bu Vigenère (Fransızca telaffuz: [[viʒnɛːʁ]](https://tr.wikipedia.org/wiki/Yard%C4%B1m:IPA)) şifre zaman geçti yeniden birçok kez. Yöntemi vardı aslında tarafından açıklanmıştır Giovan Battista Bellaso onun kaç kitap *La cifra del. Sig. Giovan Battista Bellaso*; ancak düzeni vardı sonra misattributed için Blaise de Vigenère 19. yüzyıl, ve artık yaygın olarak bilinen "Vigenère şifreleme".

Ama şifre için kolaydır, anlamak ve uygulamak için üç asır buna karşı bütün girişimleri break; bu kazandığı açıklaması, le chiffre indéchiffrable (Fransızca 'çözülemez şifre'). Birçok kişi denedi uygulamak için şifreleme programları vardır aslında Vigenère şifrelemesi. Friedrich Kasiski oldu ilk yayınlama için bir genel yöntem deşifre Vigenère şifreleme.**[6]**

**3.7. DES Algoritması**

Dünyada en çok kullanılan simetrik şifreleme algoritmalarından birisidir. Feistel şifreleme metodunu kullanır. Blok şifreleme kullanan DES, işlem sırasında 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. Anahtar uzunluğunun kısa olması nedeniyle kırılmıştır. Bunun üzerine Triple-DES, (encrypt-decrypt-encrypt)yani 3DES olarak geliştirilmiştir. 3DES, DES’in üst üste 3 kere kullanılmasıdır. Yani normal DES’e göre 3 kat yavaştır ama günümüzde SSH gibi uygulamalarda kullanılır. AES’in çıkması üzerine DES popülerliğini kaybetmiştir. Çünkü AES’e göre 6 kat daha yavaştır.**[7]**

**3.8. Diffie-Hellman anahtar değişim**

Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır. DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür. Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır. Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.**[8]**

Resim 3.1 de Diffie-Hellman Algoritmasının örneği gösterilmektedir.**[9]**

Resim 3.1 Diffie-Hellman Örneği

**3.9. RSA (Rivest-Shamir-Adleman)**

Üç bilim adamının baş harflerinden oluşan RSA, dijital imzalama içinde kullanılmaktadır. Güvenilirliği, çok büyük asal sayıların işlem yapma zorluğuna dayanan bir algoritmadır. Günümüzde bankacılık sistemleri ve ticari sistemlerde öncelikli tercih edilen şifreleme tekniğidir. Bu büyük sayılar nedeniyle oldukça güvenilirdir ama işlemler yavaştır. Bu nedenle fazla bant genişliği harcaması yüzünden kablosuz ağ sistemlerinde kullanılması bazı sorunlara yol açabilir.[10]

**3.10. (ECC) Elliptic Curve Cryptography**

Eliptik Eğri Kriptolojisi (Elliptic Curve Cryptography), sonlu cisimler üzerindeki eliptik eğrilerin cebirsel topolojisine dayanan bir açık anahtar şifrelemesidir. Eliptik eğri kriptografisinin en büyük özelliği depolama ve iletme gereksinimlerini azaltarak daha küçük anahtar boyutuna sahip olmasıdır. Bir eliptik eğri grubu, büyük modülerli ve buna bağlı olarak büyük anahtar boyutlu RSA tabanlı sistem ile aynı güvenlik seviyesi sunabilir. Örneğin; Eliptik eğri ile 256-bitlik anahtar boyutunda elde edeceğimiz güvenliği RSA ‘de 3072-bitlik anahtar ile sağlanabilir. Bu algoritma IHA’larda güvenlik açısından kullanılabilir. Ayrıca ECC smart kartlar,cep telefonları, PDA’lar (personal digital assistant), sayısal posta işaretleri gibi zorunlu ortamlara uygundur.

Bazı güvenlik sistemleri 1024-bit RSA genel anahtarlama planının uygulamasını yaymaya çalışır, çünkü kuruluşlar bunun yeterince iyi olduğunu düşünürler. Bununla birlikte bu tehlikeli bir yaklaşımdır. Çünkü genel anahtarlama sisteminin güvenliği kullanılan simetrik şifrelemeyle birebir eşleşmiş olmalıdır. Tabloda görüldüğü gibi, 1024-bit RSA simetrik şifrelemede kullanılan 128-bit güvenlik seviyesiyle uyuşmuyor.Bu gereksinimi karşılamak yani genel anahtarlama planını eşleştirmek için istenen 3072- bit RSA ya da 256-bit ECC kullanılmasıdır. Bu sayede işlemci gücü, saklama kapasitesi, bant genişliği, güç tüketimi gibi durumlarda RSA’ya göre avantaj sağlar.**[11]**

**4. Önerilen Çözümün Kısıtlamaları**

Önerilen çözümün zaman alanında bazı kısıtlamaları vardır. Bu kısıtlamalar şifreleme algoritmasının gönderilen veri içerisindeki her bir karakteri tek tek şifrelemesinden kaynaklanmaktadır ve zaman karmaşıklığı yaklaşık O(n) dir. Bu zaman kısıtını ortadan kaldırmak imkansızdır ancak daha hızlı çalışan algoritmalar geliştirmek tabiki de mümkündür.

**5.Çözüm Yöntemi**

Yaptığımız araştırmalar ve incelediğimiz başka çözümler ile edindiğimiz bilgiler sonucunda yapmayı planladığımız çözüm şöyledir. Öncelikle yapacağımız arayüz yardımı ile ceşitli kullanıcı etkileşimi sağlamamız için (yükleme, indirme, listeleme, arama, gibi..) DropBox api’larını oluşturduğumuz arayüzümüzdeki çeşitli etkileşim aletlerine implemente edeceğiz. Bunun yanı sıra verilerimizi arayüzümüzü kullanarak bilgisayarımızdan göndermeden hemen öncesinde kullanacağımız şifreleme algoritmasına göre şifreleme yapılacak ve gönderilmek istenen kullanıcıya gönderilecektir. Gönderilen kullanıcının şifreyi açabilmesi için gönderilen verimizin şifrelenirken kullanılan anahtarımızın bilinmesi gerekmektedir. Bu anahtar Diffie-Hellman anahtar paylaşım yolu ile oluşturulacak ve oluşturulan anahtar ile kullandığımız şifreleme ve şifre çözme algoritmalarımız çalışacaktır. Bunun sonucunda kullanıcılar kendi aralarında üçüncü kişilere ulaşsa bile şifreli bir şekilde erişilebilecek bir veri transferi gerçekleştirmiş olacak.

**Kaynakça**

[1] <https://tr.wikipedia.org/wiki/AES>

[2] <https://tr.wikipedia.org/wiki/Blowfish>

[3] <https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarl%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>

[4] <https://tr.wikipedia.org/wiki/Enigma_makinesi>

[5] [https://tr.wikipedia.org/wiki/Atbash#:~:text=Atbash%2C%20(%C4%B0branice%3A%20%D7%90%D7%AA%D7%91%D7%A9),bir%20anlam%C4%B1n%20%C3%A7%C3%B6z%C3%BClebilmesi%20amac%C4%B1n%C4%B1%20ta%C5%9F%C4%B1yordu](https://tr.wikipedia.org/wiki/Atbash).

[6] <https://tr.wikipedia.org/wiki/Vigen%C3%A8re_%C5%9Fifrelemesi>

[7] <https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarl%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>

[8] <https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarl%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>

[9] <https://tr.wikipedia.org/wiki/Diffie-Hellman_anahtar_de%C4%9Fi%C5%9Fimi>

[10] <https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarl%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>

[11] <https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarl%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>