Yazının icadından günümüze gizlilik her zaman ön planda olmuştur. Gizli haberleşmelerin ilk dönemlerinde şifreleme kağıt ve kalemle yapılan tekniklere dayanırken teknolojinin gelişimine bağlı olarak özellikle 1970’lerde büyük bir değişim geçiren kriptografi, günümüzde disiplinler arası (bir çok bilim dalını içeren ancak yüzde yüz bir bilim dalına ait olmayan ve kendi özerkliğini ilan etmiş bilim dalı) bir bilim dalı haline gelmiştir.

Türkiye’de 1990’lı yılların başında lisans eğitiminde seçmeli ders olarak verilmeye başlanmış, daha sonra ODTÜ ve Tübitak Marmara Araştırma Merkezi (MAM) temel bilimler grubu ortak çalışmalar yürütmüştür.

Okuma yazma yetisine sahip hemen hemen herkes hayatında az çok kod yapısı ya da şifrelerle karşılaşmıştır. Buna en basit örnek olarak anagramlar verilebilir.

Örnek : acımtırak -> acıktırma heybetli -> ehlibeyt

müşterek -> şükretme kinayeli -> enayilik

aşamalı -> aşılama bıçaklı -> balıkçı

kafiyeli -> kalifiye, kifayeli hasretli -> tarihsel

erdemli -> demirle simetrik -> kestirim

Ancak şifreler gizli ve önemli bilgiler taşıdığında bulmacalar gibi hafife alınamaz. Özellikle günümüzde kişisel bilgilerin saklanması, korunması ve iletilmesi için en önemli araç özelliğindedir. Bilgileri kodlama binlerce yıl önce devletlerin ve imparatorlukların gizli ve önemli bilgileri düşmanın eline geçmeden iletebilmesi için ortaya çıkmıştır. İletilerin kodlanması yani sözcüğün ya da cümlenin başka bir sözcük, sayı ya da sembol ile yerini değiştirerek gönderilmesi mesajların başkaları tarafından anlaşılmasını özelleştirmek içindir.

Kodların tarihteki önemi çok büyüktür. Savaşların sonucunu belirleyen, kral ve kraliçelerin ölümüne yol açan kodlar olmuştur. Bunlardan en önemlilerinden biri Queen Mary’dir. Kraliçe Mary’nin ölümü şifreli mektuplar yüzünden olmuştur. İngiltere Kraliçesi Elizabeth aynı zamanda kuzeni olan Mary’nin tahta adaylığını koymaması için bir dizi oyun çevirip onu hapse atmıştır. Hapisteyken destekleyicileriyle gizli bir şekilde yazışan Mary’nin kaçış planını içeren son mektup Elizabeth’in yaverleri tarafından deşifre edilmiş, böylece Elizabeth’in ölümü ve yerine Mary’nin geçmesi planı ortaya çıkmış, bu da Mary’nin ölümüne neden olmuştur.

Günümüzde kodların yerini şifreler almış, kod kelimesinin kullanımı azalmıştır. Sözcüklerin yerini değil, harflerin yerini değiştirerek daha temel düzeyde işlem gören şifre alternatif bir koddur. Şifrelerin kullanımı zamana göre değişiklik gösterse de mantığı değişmemiştir.

Kriptografi , Kryotos (Gizli, Saklı) ve Graphein (Yazmak ) anlamına gelen sözcüklerden türetilmiştir.

Kriptografi; gizlilik, kimlik denetimi bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler bir bilginin iletimi esnasında karşılaşılabilecek saldırılardan bilgiyi, bilgi göndericisini ve alıcısını koruma amacı taşır. Başka bir deyişle okunabilecek durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümüdür.

Kriptoloji ile ilgilenen bilim adamlarına kriptograf denir.

Kriptanaliz ise ele geçen şifrelenmiş yani anlamsız bir metinden bazı teknikler kullanarak doğru metni bulma yöntemidir. Kriptanaliz ile uğraşanlara kriptanalist denir. İyi bir kriptanalist aynı zamanda kriptografi konusunda da iyi olmalıdır. Çünkü şifrelerin nasıl tasarlanacağını bilmeyen biri nasıl çözüleceği konusunda da fikir yürütemez.

Bu iki bilimin bütününe ise kryptos (gizli) ve logos (bilim) kelimelerinin birleşimi olan kriptoloji denmektedir. Kriptoloji ile ilgilienen bilim adamlarına kriptolog denir.

1970’lere kadar kriptografi, birkaç hükümetin askeri ve diplomatik çalışanlarının bildiği, halktan gizli saklı kullanılan gizli bir teknikti. Günümüzde halen askeri alanda önemini korumaktadır. Fakat artık üniversitelerde ders olarak verilen akademik bir disiplin (bilim) haline dönüşmüştür. Diğer bir deyişle internetin. Hayatımıza girmesiyle ve bilgi dağıtım ……….. …………… …………… tüm sivil kuruluşların kullandığı, her geçen gün araştırmaların yürütüldüğü “gizli” olmaktan çıkmış bir bilim haline gelmiştir.

Kriptografinin tarihsel gelişimi içinde sanayi devrimine kadar olan süreçte karşımıza “ilkel şifreleme” yöntemleri çıkmaktadır. İlkel şifreleme yöntemleri, makineler henüz tarihte yerlerini almamışken sözcüklerin harflerinin yer değiştirmesiyle uygulanan tekniklerdir. Bu ilkel şifreleme kriptanalizin keşfiyle güvenli olmaktan çıkmış, dolayısıyla kriptograflar teknolojik gelişmelere uyum sağlayabilecek yeni şifreler geliştirmek zorunda kalmıştır. Sanayileşme ile birlikte makinelerin icadı en önemli teknolojik gelişmedir. Şifreleme işlemleri içinde geçerli olan bu icat kriptografinin yön değiştirmesi açısından önemlidir. Çünkü kağıt ve kalemin yerine ilk olarak şifre diskleri, daha sonra da bu disklerin geliştirilmiş şekli olan şifreleme makineleri (enigma) almıştır. Günümüzde ise kullanılan kuantum kriptografisidir. Kuantum kriptografisi şimdiye kadar var olan şifreleme sistemlerinden farklıdır ve bu bir sistemin bilgi güvenliğinin sonsuza dek garanti altına alınacağı yani kırılmasının imkansız olacağı iddiasına dayanmaktadır.

**TARİH BOYUNCA ŞİFRELEME VE GİZLİ HABERLEŞME YÖNTEMLERİ**

Yazının icadı insanlık tarihinin başlangıcı olarak kabul edilir. Yazıyla birlikte bilgi toplanabilir, saklanabilir ve iletilebilir hale gelmiş, dolayısıyla insanlar arasındaki iletişim kolaylaşmıştır. Zamanla toplumlar arasında ortaya çıkan çekişmeler haberleşmenin gizliliği zorunluluğunu ortaya koymuştur. Kripto tarihçisi David Khan’a göre ilk kriptografik belge M.Ö. 1900 yılında yazılan bir hiyerogliftir (antik döneme ait yazı stili) ve bu yazıt bir lordun hayatını anlatmaktadır. Aynı şekilde M.Ö. 1500’lü yıllara ait olduğu düşünülen bir Mezopotamya tabletinde çömleklerin cilalanması hakkındaki bilgilerin şifrelenmiş olarak bulunduğu görülmüştür.

Daha sonra M.Ö. 600-500 yılları arasında yaşadığı bilinen İbrani Peygamber geJenemiah’ın ATBASH şifre sistemi bilinmektedir. Bu şifre sistemi şu şekildedir. İbranice alfabesindeki ilk harf son harf ile, ikinci harf sondan ikinci harf ile olacak şekilde tüm alfabe içinde bu kurala göre yer değiştirir.

Şifreleme işlemlerinde harflerin yanı sıra sayılarda kullanılmıştır. Sayılarla oluşturulan şifreleme yöntemleri genellikle alfabedeki harflerin yerine sayılar getirilerek oluşturulur. Hemen her dilin alfabesindeki harflerin çok eskiden beri rakam olarak birer karşılığı bulunduğu bilinmektedir. Bunlar arasında en çok bilinenleri İbrani-Süryani ve Grek-Latin alfabelerindeki sistemdir. Daha sonra bu sistem Arapça içinde EBCED Hesabı olarak bilinen bir isimle kullanılmış ve Müslümanlar arasında halen kullanılmaktadır. Örnek olarak Süleymaniye ve Selimiye camilerinin görünen silüetleri 92 arşındır (1 mimar arşını 75.774 cm’dir) ve bu Muhammed kelimesinin EBCED karşılığıdır.

EBCED, Arap alfabesindeki harflerin kolay öğrenilmesi için düzenlenmiş sözcüklerdir. 8 Sözcükten oluşur. Bu 8 sözcük içinde 28 harf bulunur. İlk 9 harf 1-9’u, 2.9 harf 10-10’u ve 3. 9 harf 100-900 ve son harfte 1000’i gösterir.

Tarihteki ilk şifreleme örneklerinde ilk askeri kullanım M.Ö. 5.yy’da skytale adı verilen cihaz ile yapılmaktadır. Skytale aynı zamanda kullanılan ilk kriptografi cihazıdır. Skytale kullanarak bir mesajı şifrelemek için öncelikle uzun bir parşömen paper silindirik bir sopa etrafına sarılırdı. Gizlenecek mesaj her bir şerit turuna bir harf gelecek şekilde yazılırdı. Şerit açılıp kaldırıldıktan sonra anlamsız harflerin oluşturduğu şifrelenmiş metin ortaya çıkıyordu. Şifre çözme olayı için şifrelemede kullanılan sopa ile aynı çapta ve uzunlukta bir sopaya sahip olmak gerekirdi.

Tarihte ortaya çıkan şifrelenmiş tabletlerin yanı sıra dönemleri anlatan eserlerde de gizli yazışma tekniklerinden yararlanılmıştır. Bunlardan biri Heredotus’un yazdığına göre M.Ö. 480 yılında Yunanlılar ve Persler arasındaki savaşlarda kullanılmıştır.

Steganografi adı verilen bu yöntem Yunancada “gizlenmiş yazı” anlamına gelmektedir. Eserde şöyle anlatılmaktadır. İran’da bulunan bir Yunanlı, Yunanlılara karşı düzenlenmesi planlanan Pers istilasını kölesinin saçını kazıtarak kafa derisinin üzerine dövme ile yazmış ve kölesini saçları uzadıktan sonra Atina’ya göndermiştir. Yakalanmayan köle saçını tekrar kazıtıp mesajı iletmiş ve bu sayede Yunanlılar savaşı kazanmıştır.

Steganografi örnekleri olarak;

* Yumurta üzerine civa ile yazı yazmak
* Yazılan mesajı buruşturup balmumu ile kopyalayarak yutmak
* Limon suyu ile kağıt üzerine yazmak
* 1960’larda mor ötesi boya ile yazmak

Kaynaklardan anlaşıldığına göre kriptografi steganografinin gelişimine paralel olarak ortaya çıkmıştır. Diğer bir deyişle yazıyı saklamanın yeterli olmadığı anlaşılınca, yazıyı anlamsız sözcüklere çevirmek zorunluluk halini almıştır. Kriptografinin steganografiden farkı mesajın açıklanması değil, içeriğinin değiştirilerek anlamsız hale getirilmesidir. Steganografinin tek avantajı mesajın masun görüntülü bir ortamda olması sebebiyle dikkat çekmemesidir. Bu iki yöntemin bir arada kullanıldığı durumlarda olmuştur.

Bunlardan birincisi 2.Dünya Savaşı’nda Alman ajanları 1 sayfalık metni şifreleyip fotoğraf teknikleriyle 1mm çapında bir nokta haline dönüştürüp görünüşte önemsiz gibi görünen bir mektubun son noktası üzerine bu metni yerleştirmişlerdir. İkinci olarak özellikle PC dünyasında dijital ortamda bulunan verilerin (ses, video vb) şifrelenerek saklanmasıdır.

Tarihte Skytale’den sonra bahsedeceğimiz diğer bir kriptografi örneği Polybus’un “dama tahtası”dır. Normalde 5X5’lik bir matristir ama Türkçe’ye uygulayacak olursak 5X6’lık bir matris haline gelir.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | A | B | C | Ç | D | E |
| **2** | F | G | Ğ | H | I | İ |
| **3** | J | K | L | M | N | O |
| **4** | Ö | P | R | S | Ş | T |
| **5** | U | Ü | V | Y | Z |  |

A=11, B=12, . . . Z=55 Örnek : 46 – 52 – 43 - 32 – 26 – 54 – 16 (TÜRKİYE)

**BASİT ŞİFRELEME**

Şifreleme sistemlerinde şifrelenecek mesaja “düz metin”, şifrelenmiş mesaja da “şifreli metin” denir. Mesajın düz metin halindeki alfabesine “düz alfabe” şifre metninin yazıldığı alfabeye “şifre albafe” denir.

Basit şifreler ilkel şifreleme yöntemlerinden farklı olarak harflerin kendi arasında yer değiştirmesiyle ya da kaydırılmasıyla oluşan şifrelerdir. Mesajı gönderen ve alan önce kullanacakları şifre algoritmasına karar verir.

Örneğin kullanılacak algoritma şu şekilde olsun. Mesajın harfleri önce bir üst satıra son bir alt satıra dizilsin. Daha sonra şifrelenmiş mesaj önce üst satırdaki harflerin sonra alt satırdaki harflerin yan yana getirilip birleştirilmesi olsun.

Düz Metin : K A N T İ N D E B U L U Ş A L I M

Algoritma : K N İ D B L Ş L M

A T N E U U A I

Şifreli Metin : K N İ D B L Ş L M A T N E U U A I

Bu şekilde oluşturulan şifrelere yer değiştirme şifreleri denir. Yer değiştirme şifreleri için bir çok algoritma oluşturulabilir.

**YERİNE KOYMA ŞİFRELERİ**

Bu yöntemde düz alfabedeki harflerin rasgele karıştırılmasıyla elde edilen ve her harfin tek sefer kullanıldığı şifre alfabe ile birebir eşleştirilir.

Örneğin : Düz alfabe : A B C Ç D E …

Şifre alfabe : Ş S T U …

Yer değiştirme şifrelerinde düz metnin nasıl karıştırılacağına karar verilirken burada gönderici ve alıcının şifre alfabesinin nasıl oluşturulacağı konusunda hem fikir olması gerekir. Bu yöntem kullanılarak oluşturulan tüm olası şifre alfabe sayısı o dilin alfabesindeki harf sayısının faktöriyeli kadardır.

Kullanıldığı dönemde yer değiştirme ve yerine koyma şifreleri kırılması zor olduğu için güvenlik ve kullanım açısından pratik olmasına karşın sonraki dönemde frekans analizi denilen yöntem sayesinde kullanım dışı olmuşlardır.

Tarihteki en önemli yerine koyma şifrelerinden biri Galya savaşlarında Sezar tarafından kullanılmıştır. “Sezar şifresi” adı verilen bu şifrelemede düz alfabe yerlerinin kaydırılması söz konusudur ve bu şekilde oluşturulan şifrelere “kaydırma şifreleri” denir. Burada düz metinde bulunan her harf kendinden sonra 3. Olarak gelecek harf ile yer değiştirir.

Düz alfabe : A B C Ç D E

Şifre alfabe : Ç D E F G Ğ

Buradan görüldüğü gibi bu tarz kaydırma şifrelerinin olası şifre alfabe sayısı oldukça azdır. Örneğin Türkçe için 29 adet şifre oluşturulabilir. Bunun için modüler aritmetiği düşünmek yeterlidir. Burada M’ düz alfabedeki harfimizin sayı değeri, C, M’nin şifre alfabedeki karşılığı olsun. K kadar kaydırılmış şifre alfabe ile yazılan şifre metni için M ve C arasındaki bağıntı;

M + K = C (mod 29) şeklindedir.

Buraya kadar belirtilen örneklerde mesajı gönderen ve alan kişi algoritma üzerinde önceden bir karar vermek ve bunu güvenlikli bir şekilde saklamalıdır. Şifre algoritmasının kullandığı bazı özel bilgiler olmalı ve düşman algoritmayı bilse bile bu özel bilgileri bilmeden şifreyi çözememelidir. Bu özel bilgilere kriptografide “ANAHTAR” adı verilir. Örneğin Sezar şifrelemesinde şifre algoritması kaydırma yöntemi anahtar ise alfabedeki harflerin 3 harf sola kaydırmadır. Şifreleme ya da şifre çözme algoritması anahtar olmadan kullanılamaz ve güvenlik büyük ölçüde anahtara bağlıdır. Daha sonraki evrelerde kaydırma şifrelerinin yetersizliğinin görülmesi farklı yöntemlerin geliştirilmesi zorunluluğunu doğurdu. Bunlardan biri de önce bir anahtar belirleyip şifre alfabeyi o anahtara göre sıralamaktır.

MATEMATİK -> anahtar

MATEİKBCÇD -> algoritma

Sonuç olarak iki tarafında bu anahtar konusunda anlaşması gerekir. Anahtara sahip olmadan şifrelenmiş mesajın deşifre edilmesi bilimi olan kriptanaliz bilindiği gibi ilkel şifrelerin deşifre edilme çabası ile ortaya çıkmıştır. Bu şifrelerin zayıf yönleriyle çözülebilmesi yani daha kolay bir yoldan çözülebilmesi için matematik, istatistik ve dil bilimi alanlarında yeterli bilgiye sahip olmak gerekir.

**AL-KİNDİ VE FREKANS ANALİZİ**

Abbasi döneminde kriptanaliz için gerekli olan matematik, istatistik ve dil bilimi alanlarında önemli çalışmalar yapılıyordu. Bu bilim dallarının gelişmiş olması kriptanalizin Araplar tarafından bulunmasını sağladı ve bu alanda ilk eserler Araplar tarafından yazıldı. Bunlardan ilki 9. yüzyılda Al-Kindi’nin yazdığı “Kriptografik Mesajların Deşifresi” isimli yazıdır. Al-Kindi’nin kriptanaliz tekniğini özetlemek istersek; yazıldığı dili bildiğimiz şifreli bir mesajı çözmek için aynı dilde yazılmış yeterince uzun bir metin bulup her bir harfin kullanım sıklığını hesaplamak gerekir. Metinde en sık kullanılan harf şifreli mesajdaki en sık kullanılan harfe denk gelmektedir. Aynı işlem sırasıyla diğer harfler için de yapılır. Bu işlem bittikten sonra mesajdaki harfler ortaya çıkmış olur. Al-Kindi bu yönteme “frekans analizi” adını vermiştir [Frekans : Bir olayın birim zaman (1sn) içinde hangi sıklıkla kaç defa tekrarlandığının ölçümüdür].

- Aynı alfabeyi kullanan dillerde en çok kullanılan harfler aynı değildir.

Frekans analizini yapabilmek için şifrelenmiş metnin hangi dilde yazıldığını bilmek gerekir. Şifre sisteminde sadece harfler yer değiştirilip, dilin sahip olduğu özellikler değişmediği için şifre alfabedeki harfler yerine geçtikleri düz metin alfabesindeki harflerin özelliklerini alır. Dolayısıyla frekans dağılımına ek olarak sesli ve sessiz harflerin ilişkileri ikili ve üçlü harflerin tekrar eden durumları ve karakteristikleri kullanılarak kriptanalizde başarı sağlanabilir.

Türkçe Frekans Tablosu

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Harf** | A | B | C | Ç | D | E | F | G | Ğ | H | I | İ | J | K |  |
| **Binde** | 121 | 25 | 9 | 10 | 41 | 95 | 5 |  | 11 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

* Türkçe’de en çok karşılaşılan harf ikilileri (İN, AR, LA, AN, ER, İR, …)
* Türkçe’de en çok karşılaşılan harf üçlüleri (LAR, ARİ, BİR, DEN, NDA, …)

Bunun yanı sıra Türkçe’de bilinen büyük ünlü uyumu, küçük ünlü uyumu kuralları Türkçe bir metni analiz ederken oldukça işimize yarar, dolayısıyla frekans analizi için o dilin kurallarını iyi bilmek gerekir.

Frekans analizleri olabildiğince uzun metinlerde yapılmalıdır. Uzun metinler ya da kitaplar sayılarda çok az bir değişiklik olsa da frekans analizi yapıldığında o dilin harf frekans tablosuna uyar.

**VİGENERE ŞİFRESİ (KIRILAMAYAN ŞİFRE)**

Bu şifreleme tekniğinde birden fazla şifre alfabe kullanılır. Bu yüzden bu şifrelere çok alfabeli şifreler denir. Bilinen ilk çok alfabeli şifreleme 1518 yılında Johannes Trithemus adında bir Alman tarafından yazılan “Pollygraphic” adlı kitaptan bahsedilmektedir. Esas olarak uzun yıllar kırılamayan çok alfabeli şifreyi 1553 yılında Giovan Batista Belasa adlı bir İtalyan geliştirmiştir. O sene yayınladığı “La cifra dal sign Giovan Batiste Belasa” adlı kitabında açıkladığı bu şifre daha sonraları “Vigenere Şifresi” olarak adlandırılan şifrenin orijinal halidir. 1586’da bu şifrenin biraz daha gelişmiş şiklini tasarlayan Fransız diplomat Blaise de Vigenere adına adanan Vigenere şifresi uzun yıllar “le chiffre indechiffrable (kırılamayan şifre)” olarak adlandırılmıştır. Bu şifrenin düz metindeki her bir harf ayrı bir şifre alfabeyle şifrelenir. Hangi şifre alfabenin seçileceğine anahtar sözcüğe bakıp karar verilir. Böylece düz metindeki aynı sözcükler için farklı şifre metinler oluşur. Bu da frekans analizinin basit şifrelerdeki gibi tek başına uygulanmasına engel olur. Uzun yıllar güvenilirliğini koruyan bu şifre 1854-1863 yıllar arasında İngiliz matematikçi Charles Babbage ve Avusturya ordusunda görevli kriptograf Friedrich Kasiski tarafından kırılmıştır.

Örnek : Şifreleme işlemi için öncelikle bir anahtar harf belirlenir. “DAYI” anahtar sözcükteki her harf oluşturulacak şifre alfabenin ilk harfi olacaktır ve kaç adet şifre alfabe kullanılacağını gösterecektir.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **A** | **B** | **C** | **Ç** | **D** | **E** | **F** | **G** | **Ğ** | **H** | **I** | **İ** | **J** | **K** | **L** | **M** | **N** | **O** | **Ö** | **P** | **R** | **S** | **Ş** | **T** | **U** | **Ü** | **V** | **Y** | **Z** |
| **D** | D | E | F | G | Ğ | H | I | İ | J | K | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V | Y | Z | A | B | C | Ç |
| **A** | A | B | C | Ç | D | E | F | G | Ğ | H | I | İ | J | K | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V | Y | Z |
| **Y** | Y | Z | A | B | C | Ç | D | E | F | G | Ğ | H | I | İ | J | K | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V |
| **I** | I | İ | J | K | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V | Y | Z | A | B | C | Ç | D | E | F | G | Ğ | H |

Buna göre “ANKARA” kelimesinin şifreli hali “DNİIUA”olur.

Düz metnin ilk harfi olan “A” anahtardaki “D” harfine denk gelmektedir.

Düz metin : A N K A R A

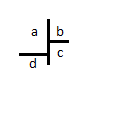
Anahtar : D A Y I D A

Şifreli metin : D N İ I U A

**1.Tamsayılar(Discret) 15.03.2017 Çarşamba**

Z={, , , , -3, -2, -1, 0, 1, 2, 3, , , , }

**2. Tamsayılar İçin Bölüm Algoritması(Öklid Algoritması )**

 1) a= b.c+d

2) a≤d<b

**3. Asal Sayı**

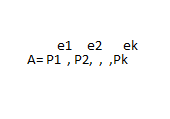
1 den büyük sadece kendisine ve 1 bölünebilen sayılardır. Asal olmayan sayılara “ Bölünebilen Sayılar “ denir.

**4.Aralarında Asal Olan Sayılar**

a ve b tamsayıları ortak böleni sadece 1 ise a ve b tamsayılarına aralarında asal tamsayılar denir.

**5.Asal Çarpanlara Ayırma**

A≥2 koşulunnu sağlayan her tamsayı k tane asal sayının çarpımı şeklinde tek olarak yazlabilir.

 P1,P2,Pk asal sayılar

e1,e2,ek pozitif tamsayılar .

**6. Modüller Aritmetik**

Modüller aritmetik bölme işlemine dayanan sayı sitemidir. Bölme işleminde bir a tamsayısının n tamsayısı ilk bölmesinde elde edilen bölüm b ve kalan k ise a= n.k+k dır.

Bölme kuralına göre 0≤k≤n-1 olur modüller aritmetik belirli bir sayıya (Modülle) göre diğer bütün sayıları o modülün kalan kümesindeki sayılarla ifade eder. Bir sayının kalan kümesi olan k {0,1,,,,,,,n-1}’dir. Bir sayının n ile bölümünden kalan sayı o sayının modülüne denk olduğu sayıdır. Yani a≡k(mod n) şeklinde gösterilir.

Kalan kümesindeki sayılar modülündeki sayılar birden fazla sayıya denktir.

Örneğin 13≡1(Mod 3), 28≡1(Mod 3)

Dolayısıyla kalan kümesindeki her eleman belirlediği denklik sınıfının temsilcisi olaarak alınırsa n sayısının denklik sınıfları.

O,1,2……….(n-1)’dir. (not üst çizgi var )

Bu denklik sınıflarının kümesi 2^n olarak gösterilir.

z^n= {0,1,2, , , ,(n-1)}

z^3={0,1,2}

O={, , , -6, -3, 0, 3, 6, , , }

1.={, , ,-3, -2, 1, 4}

**7. Matris Çarpımı**

A= ve B= z/n’de verilen 2x2 tipinde iki matris olsun.

A X B=

**8. Matrisin Tersi**

S= z/n’ de 2x2 tipinde bir matris. Bir matrisin tersinin olabilmesi için.

a.d-b.c≠0 olması gerek(gerek ve yeter şart)

det S(a.d-b.c) ≠0 S^-1=det^-1.

**Örnek**

S= matrisin z/zg de tersi varmıdır bulunuz.

Det s(2.5-4.3)mod=-2. Det S^-1.detS= 1(Mod 29) detS^-1 pozitif olacak

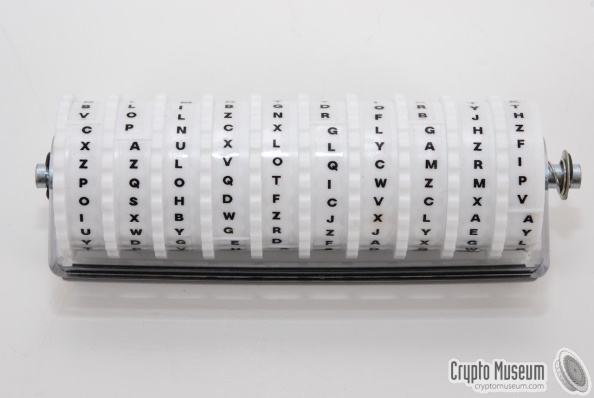
S^-1=14 S^-1=

S^-1=

**THOMOS JEFFERSON, JEFFERSON DİSKİ(1790)**

18. yüzyılın sonlarına kadar Vigenere şifresinin üstünlüğü devam etse de diğer yandan  yeni sistemler de üretilmesi içinde yoğun çaba harcanıyor. 1790 yılında Thomas Jefferson, Pennyslvainia üniversitesi matematikçilerinden Dr. Robert Patterson’un yardımıyla şu anda Jefferson Diski adıyla bildiğimiz sistemi geliştirdi.  Bu disk İngiliz alfabesinin harf sayısı nedeniyle toplamda 26 diskten oluşmaktaydı. Her disk üzerinde alfabedeki tüm harfler rastgele biçimde yazılmıştı. Şifreleme işlemini yapmak isteyen kişi düz metni Jefferson diskindeki bir sırada oluşturup geri kalan sıralardan herhangi birini seçerek şifre metni elde ediyordu. Aynı özellikleri taşıyan Jefferson diski hem alıcıdan hemde gönderici tarafında bulunmak zorundaydı. Dolayısıyla her Jefferson diski aynı değildi ve bu yüzden güvenilir bir sistem oluşturmuştur.

Bu şifreleme aletinin benzeri 2. Dünya Savaşı’nda Amerika ordusu tarafından kullanılmıştır. Tasarladığı bu sistem ile Jefferson Amerikan kriptografisinin babası olarak anılmaktadır.

Böyle bir şekli var 1 tane anlamlı kelime kısmı oluyor ve diğerleri anlamsız oluyor.Anlamsız belirleniyor şifre ona göre oluşturuluyor.

**CHARLES WHEATSONE, WHEATSONE-PLAYFAİR ŞİFRESİ(1854)**

Adını Charles Wheatsone ve Baron Liyan Playfair ‘den alan bu şifre Polybius dama tahtası gibi 5x5’lik bir matris kullanmaktadır. Aslında bu şifreleme biçimi 26 harften oluşan İngiliz alfabesi için tasarlanmış I ve J harfleri bir arada düşünülerek 25 hücresi olan bir matris ortaya koyulmuştur. Playfair şifresinde şifreleme algoritması düz metindeki her bir harf çifttini başka bir harf çifti ile değiştirir. Fakat şifreleme işlemine geçmeden önce bir anahtar belirlenmesi ve o anahtara göre matrisin oluşturulması gerekir.

Anahtar matrisin ilk hücresinden başlayarak her hücreye bir harf yazılacak şekilde 1. Satırdan yazılmaya başlanır. 1’den fazla kullanılan harfler ilk kullanımından sonra atılır. Ve ilk satıra sığmadığı takdirde 2. Satırdan devam edilir. Anahtar yazılıp kalan hücrelerde alfabenin geri kalan harfleri sırayla yazılır.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | R | İ | P | T |
| O | G | A | F | B |
| C | Ç | D | E | Ğ |
| H | I | J | L | M |
| N | Ö | (S/Ş) | (U/Ü) | (V/Y/Z) |

Algoritma işleyişi şu şekilde olsun;

**1)** İkilideki harflerden 2 si de aynı satırda ise sağlarındaki harflerle yer değiştirirler. Eğer harflerden biri satır sonunda olursa o zaman satır başındaki harfl ile yer değiştirme yapılır. Örnek: “SÜ” “UV”

**2)** İkilideki harflerden 2 si de aynı sütunda ise altlarında bulunan harfler ile yer değiştirme yapılır.

Örnek: “AS” “Dİ”

**3)** İkilideki harfler aynı satırda veya aynı sütunda değil ise ilk harfi şifrelemek için bu harfin bulunduğu satır ve 2. harfin bulunduğu sütunun kesişimindeki harf alınır. 2. harfi şifrelemek için ise ilk harfin bulunduğu sütun ve ikinci harfin bulunduğu satırın kesişimindeki harf alınır.

Örnek: “MA” “JB”

ÖRNEK: ACPVVNFÖJFJBMJJBPĞJBKPPCÖUKPPVUV Kriptograf tablosuna göre düz metin halini bulunuz.

ODTÜ UYGULAMALl MATEMATİK ENSTİTÜSÜ sonucunu elde ederiz. (Bu örneği tersten uyguladığımız için yani şifreden düz metne geçtiğimiz için mesela aynı satırda bulunanların sağlarındaki harflerle değil sol tarafttaki harfler ile yer değiştirmeleri gerekmektedir.)

**AUGUSTE KERCKHOFFS VE PRENSİPLERİ**

Bir şifre sisteminin sağlanması gereken en önemli özelliği güvenli ve pratik olmasıdır. Bu konuyu ilk kez Hollandalı dil bilimci Auguste Kerckhoffs yazılı hale dökmüş. 1883 de yayınladığı makalesinde bir şifreleme sisteminde anahtar bilinmediği takdirde sistem ile ilgili her şey bilimsel ile sistemin güvenliğinin tam olması gerektiği ifade edilmiştir. Kerckhoff prensipleri bu tarihten sonra tasarlanan şifre sistemleri için önemli yol gösterici olmuştur. Prensipleri 6 ana maddede toparlar isek;

1)Sistem pratik ve matematiksel bir gerçekliğe dayanmakta.

2)Sistem gizliliğe dayanmamalı yani herkes sistem ile ilgili her şeyi bilmeli.

3)Sistemde kullanılan anahtarlar taraflar arasında ve 3. Kişinin değiştirmesine izin vermeden değiştirilebilmeli.

4)Sistem telgraf uygulamasında kullanılabilmeli.

5)Sistemin kullanılabilmesi için fazla sayıda insana ihtiyaç duyulmalı.

6)Sistemin uygulanması ve anlaşılması kolay olmalı ve şifreleme sisteminin güvenliği şifreleme algoritmasını gizli tutmaya dayanmamaktadır. Güvenlik yalnızca anahtarı gizli tutmaya dayanmaktadır.

Burada 2. Madde Krechoff prensibi olarak bilinir ve işi “bir kripto sistemin güvenliği anahtarın gizliliğine bağlıdır”

Şeklinde özetler.

**LESTE S.HİLL VE HİLL ŞİFRELENMESİ(1929)**

Çok alfabeli şifreleme sistemlerinin bir örneğidir. Ve çok alfabeli şifreleri daha pratik hale getirmesi yönünden çok önemlidir. Lineer cebire dayanmaktadır. Şifrelenmek istenen düz metin alt gruplara bölünerek önceden belirlenmiş anahtar matrisler ile işleme sokulur. Bu nedenle harflerin sayılara çevrilmesi gerekir. Hill şifresi için öncelikle alfabedeki her harf bir sayıya karşılık gelir.

ABCÇ……………K………….Z

0123……………13………..28

Hill şifresinin pratikteki kullanımı düz metni 2’li bloklar halinde şifrelemektir.

Örnek: Düz metin=GECE

Anahtar=Her iki tarafında belirlediği Z/29’da tersi olan matris seçelim.

S= olsun. Şifreli metni bulalım.

G E C E

7 5 2 5 OLUR.

olarak gösterilir.

.= ise CY ye karşılık gelir.

.= ise NŞ ye denk gelir. O zaman şifreli metnimiz “CYNŞ” olur.