2020/2021 EĞİTİM ÖĞRETİM YILI MATEMATİK PROJESİ

ÖĞRENCİNİN:
AD: ÖMER
SOYAD: ERBOĞA
SINIF:11/B
NO:329

KONU:
KRİPTOGRAFİ NEDİR?

KRİPTOGRAFİ

Kriptografi (kriptoloji, Yunanca kryptos “gizli” ve grafo “yazmak” fiilinden türetilmiştir), mesaj gizliliği çalışmasıdır. Günümüzüde, bilginin matematiksel çalışması ve özellikle bir yerden başka bir yere taşınması olarak bilişim kuramının bir bölümü olmuştur.

Kriptografi ya da ‘şifreleme’ okunabilir bir durumdaki verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür. Kriptografi bir matematiksel yöntemler bütünüdür ve önemli bilgilerin güvenliği için gerekli gizlilik, aslıyla aynılık, kimlik denetimi, ve asılsız reddi önleme gibi şartları sağlamak amaçlıdır. Bu yöntemler, bir bilginin iletimi esnasında ve saklanma süresinde karşılaşabilecek aktif saldırı ya da pasif algılamalardan bilgiyi koruma amacı güderler.

ŞİFRELEMENİN TEMEL AMAÇLARI

- GİZLİLİK: Gizli kalması gereken bilgilerin, başka kişilerin eline geçmesini engellemektir.
- KİMLİK DENETİM: Şifreleme yapan kişi ile çözen kişi bellidir. Şifreleme kullanılmasaydı, mesajı aynı isimle herhangi biri iletebilirdi.
- BÜTÜNLÜK: Orijinal mesajın gönderildiği gibi olduğunu, üzerinde hiçbir değişiklik, ekleme, çıkarma ve yeniden düzenleme yapılmadığını garanti altına almaktır.
- REDDEDİLMEZLİK: Gönderen mesajı gönderdiğini, alıcı ise aldığını inkar edemez.
- ERİŞİM KONTROLÜ: İzinsiz kişi ya da uygulamaların erişmemeleri gereken kaynaklara erişmelerini engellemesidir.

KRİPTOLOJİ

Kriptoloji, şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletişim mesajının deşifre edilmesidir.

Günümüz teknolojisinin baş döndürücü hızı göz önüne alındığında, teknolojinin gelişmesiyle birlikte ortaya çıkan güvenlik açığının da taşıdığı önem ortaya çıkan güvenlik açığını da taşıdığı önem ortaya çıkmaktadır. Kriptoloji; askeri kurumlardan, kişiler arası veya özel devlet kurumları arasındaki iletişimlerden, sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır.

Kriptoloji = Kriptografi + Kriptoanaliz. Kriptoloji bilimi kendi içerisinde iki farklı branşa ayrılır. Bunlar Kriptografi; şifreli yazı yazma ve Kriptoanaliz; şifreleri çözme ya da analiz etmedir. Kriptoloji, çok eski ve renkli bir geçmişe sahiptir.

K**RİPTOGRAFİ TARİHİ**

Kriptoloji çok eski çağlardan beri insanoğlu tarafından kullanılmaktadır. Bu tarihçeye kısaca bakacak olursak:

- MÖ.1900 dolaylarında bir Mısırlı katip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı.
- MÖ.60-50 Julius Caesar normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yönetimini devlet haberleşmesinde kullandı. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu.
- 725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı (Bu kitap kayıp durumdadır). Kitabı yazmasına ilham kaynağı olan, Bizans imparatoru için Yunanca yazılmış bir şifreli mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır.
- 1000-1200 Gaznelilerden günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu.
- 1586 Blaise de Vigenere (1523-1596) şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin içim otomatik anahtarlama yönteminden bahsedildi. Günümüzde bu yöntem hala DES CBS ve CFB kiplerinde kullanılmaktadır.
- 1623'de Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografi buldu.
- 1790' da Thomas Jefferson, Strip Cipher makinesini geliştirdi. Bu makineyi temel alan M-138-A, ABD donanmasının 2.Dünya savaşında da kullanıldı.
- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.
- 1985'de Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif ettiler
- 1990'da Xuejia Lai ve James Massey: IDEA algoritmasını buldular.
- 1991'de Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı.

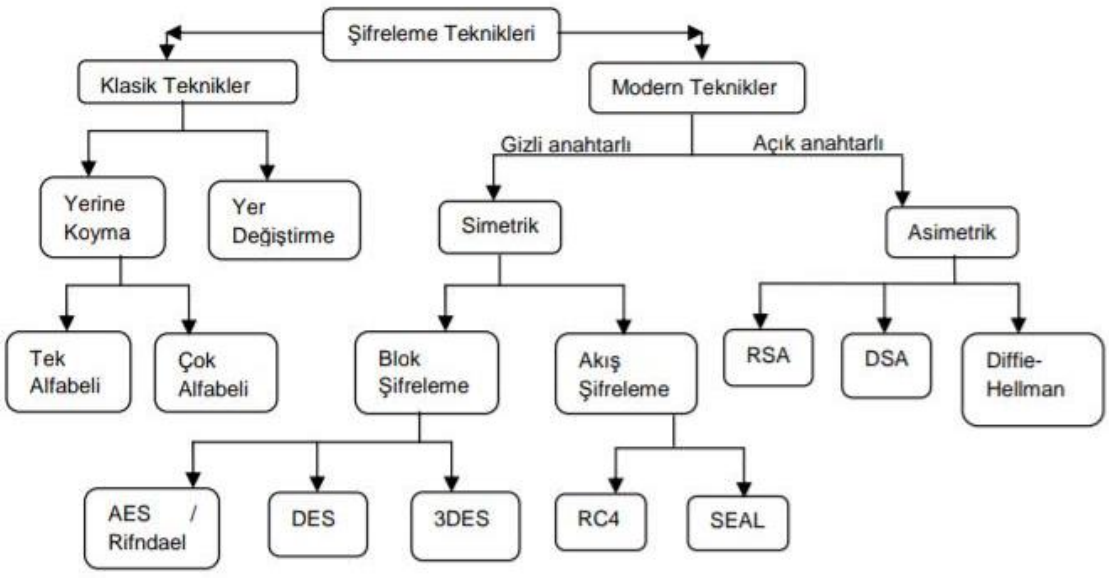
- 1995’de SHA-1 (Secure Hash Algorithm) özet algoritması NIST tarafından standart olarak yayınlandı.
- 1997’de ABD’nin NIST (Natioanal Institute of Standartds and Technology) kurumu DES’in yerini alacak bir simetrik algoritma için yarışma açtı.
- 2001’de NIST’in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen ‘e ait Rijndael algoritması, AES (Advanced Eneryption Standard) adıyla standart haline getirildi.

KULLANIM ALANLARI

Kriptoloji; askeri kurumlardan, kişiler arası veya özel devlet kurumları arasındaki iletişimlerden, sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır.

KRİPTOGRAFİ ALGORİTMALARININ SINIFLANDIRILMASI

Gelişen teknoloji ile şifreleme için uygulanan yöntemler de farklılık göstermiştir Kriptografi algoritmaları klasik ve modern olmak üzere iki ana kategoriye ayrılabilir.



KLASİK TENİKLER

Klasik şifreleme teknikleri daha çok kağıt ve kalem kullanılarak gerçekleştirebilecek algoritmalardır. Elektronik bilgisayarlar ortaya çıkmadan önce kullanılmışlardır.

Klasik kriptografi sadece askeri işlemlerde ve ileri akademik kurumlarda kullanılmıştır. Klasik teknikler, algoritması gizli olan şifreleme tekniklerini içermektedir. Algoritmanın gizli tutulması gerektiği için güvenirliği düşük algoritmalardır.

Sezar, playfair, hill, viegenere, ENGİMA sistemleri klasik tekniklerden bazılarıdır.

SEZAR ŞİFRELEME

Alfabedeki harflerin sıra numaraları belirli bir miktar kaydırılarak şifreli karşılıkları elde edilir. Tek alfabeli şifreleme tekniğidir. Bu teknik öteleme şifrelemesi olarak da bilinir. Eğer harflerin ötelenme miktarı üç olursa Sezar şifreleme tekniği olur. Eğer öteleme şifresi Türkçe Alfabe için kullanılacaksa bu değer 29 olmalıdır.

Örneğin;

a b c d e f g ğ h ı i j k l m n o ö p r s ş t u ü v y z
0 1 2 3 4 ……26 27 28

ALBERTİ DİSKİ

1404-1472 yılları arasında yaşamış olan Leon Alberti, 1466-1467 yılları arasında ilk kez çoklu alfabe kullanarak kriptolama yapmıştır. Bu yöntemde, Sezar şifreleme yöntemine benzer olarak harf kaydırma tekniği uygulanmıştır. Sezar şifrelemeden farklı olarak kaydırma miktarı sabit olmayıp, kullanıcının kararına göre belirlenmektedir. Kriptolanacak metinde her harfin kriptolu karşılığı, Alberti Diski yardımıyla bulunmaktadır. İçteki çemberi sabit, dıştaki çemberi onun etrafında dönebilen bu disk yardımıyla, her harfin istenilen miktarda ötelenmiş hali kolaylıkla görülebilmektedir.

VİEGENERE ŞİFRELEME

1553 YILINDA Giovan Batista Belaso adlı bir İtalyan uzun yıllar kırılamayan çok alfabeli şifreyi geliştirmiştir. 1586'da bu şifrenin biraz daha gelişmiş şeklini tasarlayan ve sunan Fransız diplomat Bliase de Vigenere'den dolayı Vigenere şifresi adını almıştır. Bu teknikte düz metindeki her bir harf ayrı bir şifre alfabeyle şifrelenir. Şifre alfabenin seçiminde anahtar kelimeye göre karar verilir. Anahtar kelimenin farklı seçilmesi, düz metindeki aynı kelimeler için farklı şifreli metinler oluşmasını sağlar. Bu durum frekans analizinin tek alfabeli şifreleme tekniklerindeki gibi iyi sonuç vermesini engeller. Uzun yıllar güvenirliğini koruyan bu şifre 1854-1863 yılları arasında İngiliz matematikçi Charles Babbage ve Avusturya ordusunda görevli kriptograf Friedrich Kasiski tarafından kırılmıştır.

VERNAM ŞİFRELEME

1917 yılında Gilbert Vernam tarafından geliştirilmiştir. Telgraf hatlarındaki haberleşmenin şifrelenmesinde kullanılmıştır. Vernam şifreleme tekniği Vigenere şifreleme tekniğine benzer. Farkı ikili sayı sistemini (0 ve 1) kullanması ve düz metinin XOR (exclusive-or) işleminden geçmesidir. Rastgele belirlenen kendisini tekrarlamayan anahtar dizisi ile şifreleme işlemi yapılır. Şifreleme işleminde ikili sayı sisteminde yazılmış Baudot adı verilen 5 bitlik karakter dizileri kullanılır. Her harf için Baudot kodu farklıdır. Rastgele belirlenen anahtar dizini her bir karakterine karşılık gelen Baudot koduna düz metinin her bir karakterinin Baudot kodu eklenerek (XOR) yeni şifreli karakter dizisi elde edilir.

HİLL ŞİFRELEME

Hill şifrelemede şifreleme anahtarı olarak bir katsayılar matrisi (K) kullanılır. Katsayılar matrisinin elemanları ile düz metindeki karakterlerin sayısal karşılıklarından elde edilen matrisin elemanları çarpılır. Düz metin uzunluğu 2 birim olan kaakter gruplarına ayrılır. Düz metinin uzunluğu d=2, düz metin m1m2, şifreli metin c1c2 olmak üzere katsayılar matrisisin eleman sayısı 4'tür.

PLAYFAİR ŞİFRELEME

Bu teknik adını İngiliz bilim adamı Lyon Playfair'den almıştır. Yerine koyma yönteminin bir türüdür. Şifreleme tekniği 1854'te Charles Wheatstone bulmuştur, Lyon Playfair geliştirmiştir. Bu teknik Birinci Dünya Savaşı'nda İngilizler tarafından kullanılmıştır. 5x5'lik matris düzeni ile şifreleme işlemini gerçekleştirir.

ENİGMA

Enigma İkinci dünya Savaşı döneminde Almanlar tarafından kullanılmıştır. Düz metinleri mekanik ortamda şifrelemek için geliştirilen bir makinedir. Enigmada 26 harften oluşan bir klavye bulunmaktadır. Şifreleme işlemini hareketli olan üç adet şifreleme çarkı ve hareketsiz olan bir adet çark gerçekleştirir. Sabit olan çark yansıtıcı çark olarak adlandırılır. Hareketli çarkları ters düz eden bir mil kullanılır. Hareketli çarkların kenarlarında alfabenin harfleri vardır. En üstteki harfler küçük bir kapaktan görülebilir. Hareketli olan her çarkın bir yüzüne 26 ortak merkezli sabit bağlantı diğer yüzüne 26 yaylı bağlantı yerleştirilir. Sabit ve yaylı bağlantıların birbiri ile yalıtımlı kablolar aracılığı sayesinde düzensiz olarak iletişim kurması sağlanır. Sabit çark üzerinde sadece yaylı bağlantılar vardır ve bu bağlantılar düzensiz olarak çiftler halinde birbirleri ile bağlanmıştır. Enigma şifreleme makinesinin esas gizemi dört çark arasında kablolar ile sağlanan iletişimdir. Seçilebilicek 26 harf için 26 kablo yuvası bulunur ve her bir kablo 2 yuvaya takılır.

MODERN TEKNİKLER

Bilgisayar sistemlerinin gelişmesi ile şifreleme sistemleri bilgisayar programları ile gerçekleştirilmeye başlanmıştır. Modern teknikler kağıt-kalem sistemlerinden daha karmaşık yapıya sahiptir. Harflerin elektronik ortamda bitlerle ifade edilmesi sonucu şifreleme işlemleri bitlerle yapılmaya başlanmıştır. Genel olarak simetrik algoritmalar, asimetrik algoritmalar ve hash algoritmalar olmak üzere üç sınıfta incelenmektedir.

SİMETRİK(GİZLİ ANAHTARLI) ŞİFRELEME TEKNİKLERİ

Tek bir anahtar kullanılır. Aynı anahtarla hem şifreleme işlemi hem de şifreyi çözme işlemi yapılır. Bu nedenle simetrik şifreleme sistemlerinde şifreleme işleminde kullanılan anahtar gizlidir. Anahtar bilgisi sadece metini gönderen ve alan kişilerde olmalıdır. Anahtarın başka kişilerce bilinmesi iletilecek metinin güvenliği tehlikeye atar.

ASİMETRİK (AÇIK ANAHTARLI) ŞİFRELEME TEKNİKLERİ

Asimetrik şifreleme tekniklerinde iki farklı anahtar kullanılır. Birinci anahtar şifreleme işleminde kullanılır ve herkese açıktır. İkinci anahtar ise şifreyi çözme işleminde kullanılır ve sadece şifreli metini açması gereken kişiye özeldir.

HASH ŞİFRELEME TEKNİKLERİ

Özetleme işlemi yaparlar. Mesajdan sabit uzunlukta bir dizi üretilir ve buna mesaj özeti denir. Üretilen özet metnin karakterini taşır. Şifrelenecek metindeki tek bir karakter değişikliği üretilecek özette büyük değişikliklere yol açar. Hash algoritmalarda özetleme tek yönlü olduğu için özetten asıl metine dönüş yapılamaz. Yakın geçmişte modern tekniklere hibrid ve kuantum teknikler olmak üzere yeni algoritmalar eklenmiştir.

HYBRİD ŞİFRELEME TEKNİKLERİ

Simetrik ve asimetrik şifreleme tekniklerinin birlikte kullanılması ile ortaya çıkmıştır. Her iki yöntemin üstün yönlerini birleştirerek zayıf yönleri ortadan kaldırmayı amaçlar. Hybrid sistemlerde düz metinin şifrelenmesi işlemi simetrik algoritmalarla yapılır. Şifreleme anahtarı ise asimetrik algoritmalarla gizlenir. Mesaj ve anahtar bir arada karşı tarafa iletilir. Bilginin simetrik algoritma ile şifrelenmesi işlemlere hız kazandırırken, anahtarın asimetrik algoritma ile gizlenmesi güvenliğini artırır.

KUANTUM ŞİFRELEME TEKNİKLERİ

Tek kullanımlık anahtar kriptografi tekniğidir. Güvenli ve devamlı anahtar dağıtımını garantiler. Kuantum mekaniğine ait belirsizlik ilkesi, foton polarizasyonu, dolaşıklık gibi yasalardan yararlanır.

KRİPTOGRAFİ ÖRNEKLERİ

Örnek 1:

Farzedelim ki mesaj y=(11x+4)MOD26 fonksiyonu ile şifrelensin.Şifreli metnimiz MONEY.

Öncelikle düz metnimizde ki her bir karakterin aşağıda verilen listedeki olduğu gibi 0 ile 25 arasındaki sayısal değerlerini bulmalıyız.

A-0 B-1 C-2 D-3 D-3 …… Y-24 Z-25

Böylece MONEY metnimizin uygun sayısal değerleri 12, 14, 13, 4 ve 24 tür.

Buradaki her bir değer için daha önce belirlediğimiz y=(11x+4)MOD26 fonksiyonunu kullanırsak.

M: y =(11*12+4)MOD26=6 —-G

O: y =(11*14+4)MOD26= 2 ——C

N: y=(11*13+4)MOD26=17 ——R ➡ Böylece bulduğumuz şifreli metnimiz “GCRWI” olur.

E: y=(11*4+4)MOD26=22 ——W

Y: y=(11*24+4)MOD26=8 ——I

Şifre çözümü:

Şifre çözümü (deşifreleme) için y fonksiyonunu aşağıdaki gibi değiştirelim.

=(ters(a)(y-b)MODm deşifreleme fonksiyonumuza=11 ve b=4 demiştik. Böylelikle x=ters(11)(y-4)MOD26yı elde edebiliriz. Ters(11)MOD26=19 ve bu şekilde deşifreleme fonksiyonumuz x=19(y- 4)MOD26 olur. Şimdi şifreli metnimiz olan “GCRWI” deki her bir karakterin karşılığı olan sayısal değeri tablomuzdan bulalım. 6,2,17,22,8 dir.

G: x=19*(6-4)MOD26=12 ——M

C: x=19*(2-4)MOD26=14 ——O

R: x=19*(17-4)MOD26= 13 —-N → Bu sayede düz metnimize ulaşırız “MONEY

W: x=19*(22-4)MOD26=4 ——E

I: x=19*(8-4)MOD26=24 ——Y

Örnek 2 :Sezar şifreleme sisteminde, “SEZAR” açık yazısı, Türkçe alfabede, hangi gizli yazıya dönüşür?

A-)RDYZP %10

B-)UĞCÇT % 20

C-)ŞFABS %40

D-)BRÜTÜS %30

ÇÜNKÜ SEZAR ŞİFRELEME SİSTEMİNDE TEMELİ VERİLEN HARFİN 3 KONUM SONRAKİ KARŞILIĞI İLE DEĞİŞTİRİLEREK ŞİFRELENİR

Örnek 3:Aşağıda verilen açık yazılar ve verilen anahtarlarla, oluşan gizli yazıların anlamlı hale gelen kelime karşılığını bulacağız.

Bu sorumuzu çözerken A = 0, B = 1, C = 2, …, Z = 28 kodlamasını kullanacağız

Açık Yazı	Anahtar	Gizli Yazı		Açık Yazı	Anahtar	Gizli Yazı
DÜNYA	KALEM			DÜNYA	KALEM	OÜBÇM
TELEFON	SM			TELEFON	SMS	MRFVSHĞ
MAKİNE	ÖEŞJÖM			MAKİNE	ÖEŞJÖM	DEFTER
ARNAVUTLUK	TİRAN			ARNAVUTLUK	TİRAN	TCGAKÖEEUA
TONTON	ÜJE			TONTON	ÜJE	PASPAS

AÇIKLAMA:

AÇIK YAZI: D=4 Ü=25 N=16 Y=27 A=0

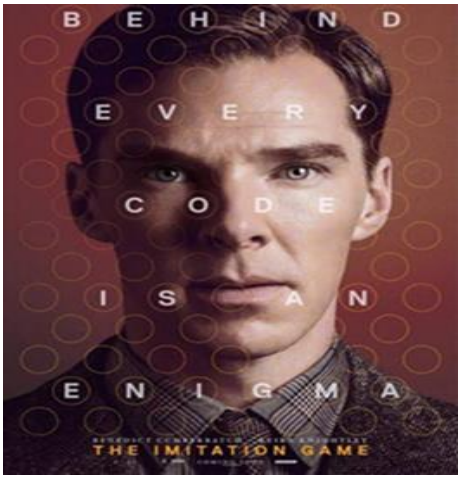
ANAHTAR KELİME: K=13 A=0 L=15 E=6 M=15

=> 17=25=31=33=16 Buda harf değerleri olarak O-Ü-B-Ç-M olarak den gelmektedir

KRİPTOGRAFİ KONULU FİLM VE KİTAPLAR

Da Vinci'nin Şifresi: 2006 yılında vizyona giren Dan Brown'ın aynı adlı eserinden uyarlanan Da Vinci'nin Şifresi adlı filmin baş kahramanı Robert Langdon'dır. Film, Leonardo Da Vinci'nin duvar resmi olan Son Akşam Yemeği'nde, Kutsal Kase'nin, Steganografi tekniği ile gizlenmiş olduğunu düşünen kahramanı konu alır.

Enigma: Micheal Apted tarafından yönetilen bir casusluk gerilim filmidir. Senaryosu Robert Harris'in Enigma adlı romanından uyarlanan film, İkinci Dünya Savaşındaki Enigma kod kırıcılarını konu alıyor. Enigma, mesajların şifrelenmesi ve şifrelerin çözümlenmesi için kullanılan bir şifreleme makinasıdır. Hikaye son derece kurgusal olmasına rağmen, 2.Dünya Savaşı sırasında Alman mesajlarını şifreleme ve Enigma ile şifresini çözme süreci ayrıntılı olarak ele alınmakta ve Katyn katliamının tarihsel olayı vurgulanmaktadır.



KAYNAKÇA:

1. https://cod3xblog.wordpress.com/
2. https://www.iienstitu.com/blog/kriptografi-nedir-teknikleri-nelerdir
3. https://openaccess.maltepe.edu.tr/
4. https://tr.wikipedia.org/
5. https://dspace.gazi.edu.tr/
6. https://dkocausta.medium.com/