AMAÇ : Bu uygulamanın amacı kişiye doğal dillerde var olan her harfin farklı frekans değerine sahip olduğunu göstermek, Türkçe de bulunan harflerin frekans tablosunu oluşturabilmesini sağlamak ve bu veriler üzerinden basit dizi şifreli algoritmalar harf frekans değer tablosuna dayanarak kriptanaliz edebilmesini katkıda bulunmaktır.

ÖNBİLGİ :

Frekans Tabloları : Her dilde harflerin kelimelerde ortalama kullanım oranları farklılık göstermektedir. Bazı harfler çok sık kullanılırken bazıları daha az kullanılmaktadır. Bu amaçla diller için harf kullanım frekansları tabloları oluşturulmuştur. Bu frekanslar şifreli metin ile açık metin arasında bağlantı kurup şifreli metnin çözülmesinde kullanılmaktadır. Dillere göre harf kullanım sıklık oranları aşağıda verilmiştir.

İNGİLİZCE	E T A O I N S H R D L C U M W F G Y P B V K J X Q Z
ALMANCA	E N I S R A T D H U L G C O M W B F K Z Ü V P Ö Ä ß J Y X Q
İSPANYOLCA	E A O S R N I D L C T U M P B G V Y Q H F Z J X W K
FRANSIZCA	E S A I T N R U L O D C P M É V Q F B G H J À X Y È Ê Z W Ç Ù K Î Œ Ï Ë
TÜRKÇE	

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

a) Türk_alfabesinde_harflerin_frekans_tablosu (Türkçe_sözlük) → harf frekans tablosu

Türk Dil Kurumunun web sayfasında bulunan Türkçe kelimeler ekte paylaşılmıştır. Türkçe sözlüğü parametre olarak alan ve bize bu sözlükteki harflerin kullanım sıklığına (harfin kullanım sayısı/sözlükte kullanılan tüm harflerin toplam kullanım sayısı) göre Türk alfabesinde kullanılan harflerin kullanım frekans değer tablosunu kullanım oranın büyüklüğüne göre büyükten küçüğe doğru sıralanmış halini geri döndüren bir fonksiyon tasarlayıp, kodlayınız. Bu fonksiyona göre aşağıdaki değer tablosunu doldurunuz.

Tablo 1 Türk Alfabesinde Bulunan Harflerin Türk Dilindeki Frekans Tablosu

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

B. Uygulamanın Yapılışı:

a) 1. Nolu uygulamada tasarlanan şifreleme fonksiyonu ile sizinle lab çalışmasında paylaşılan Türkçe metnin şifreleyin. Şifrelenen Türkçe gizli metni, uygulama öncesi oluşturulan Türkçe harf frekans tablosu kullanılarak kriptanalizini gerçekleştirin. Şifrelenen metin için kısa ve uzun metinler kullanarak sonuçlarını gözleyin.

b) Cryptool-online sanal yöresinde verilen metin için n-gram analizi yaparak, sonuçları gözlemleyin.

c) Sizi verilen Türkçe sözlüğü kullanarak Türkçe diline ait iki, ve üç gram tablosu oluşturun.

Tablo 2 Türk Diline Ait n-gram Tablosu

Nr.	Histogram			Bigram			Trigram		
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									
12.									
13.									
14.									
15.									
16.									
17.									
18.									
19.									
20.									
21.									
22.									
23.									
24.									
25.									
26.									
27.									
28.									
29.									

ANALİZ :

- Uzun ve kısa metin frekans analiz işleminizi nasıl etkiledi?

- Harf tabanlı frekans tespitinde metin uzunluğu olarak kırılma noktanız nedir?

- Term frequency ve n-gram analiz zaman ve doğruluk değerleri açısından karşılaştırın.

- Verilen metnin hangi dile ait olduğunu frekans analizi ile bulunabilir mi?

- n-gram ve frekans analizine karşı daha dirençli kriptografi yöntemleri için neler yapılabilir tartışınız.

REFERANSLAR :