AMAÇ : Bu uygulamanın amacı kişiye kriptolama, gizli ve açık anahtar, şifreleme ve deşifreleme yöntemlerinin genel çalışma yapısını göstermek ve kişinin bu prensiplere dayalı basit gizli anahtar yapısıyla çalışan tek ve çok alfabeli şifreleme uygulamaları oluşturabilmesi sağlamaktır. Uygulama kapsamında kişinin basit sezar şifreleme ve deşifreleme ile mors dönüşüm işlemleri yapabilmesi beklenmektedir.

ÖNBİLGİ :

Şifreleme /deşifreleme : Açık şekilde bulunan bir metnin (plaintext) belli işlemler uygulanarak anlamsız hale getirilip şifreli metne dönüştürülmesine **şifreleme**, şifreli metnin tekrar eski açık metin haline dönüştürülmesi **deşifreleme** olarak adlandırılmaktadır. Şifreleme ve deşifreleme işleminde amaç açık metin ile şifreli metin arasındaki ilişkiyi en aza indirmektir. Dönüşüm işlemlerinde kullanılan bu **transformasyon işlemleri tersinirdir**. Bu nedenle şifreli bilgiden açık metnin elde edilmesini önlemek için şifreleme ve deşifreleme algoritmasının gizli tutulması gerekmektedir. Yalnızca mesajlaşan kişilerin bilebileceği bir gizli anahtarın şifreleme ve deşifreleme işlemlerinde kullanılması şifreli mesajlaşmada en önemli kriterin kullanılan anahtarın gizliliği olmasını beraberinde getirecek ve şifreleme ve deşifreleme yöntemlerinin gizli tutulması zorunluluğunu ortadan kaldıracaktır.

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

Kriptografi, açık metin, şifreli metin, şifreleyici, anahtar, şifreleme, deşifreleme, kripto analiz, kriptoloji kavramları üzerine bilgi sahibi olmanız beklenmektedir.

Şifreleme_deşifreleme (açık_metin, mod= (şifrele, deşifrele)) → şifreli_metin

Açık metni ve yapacağı şifreleme yada deşifreleme modunu parametre olarak alan ve şifreli metin üreten bir fonksiyon dizayn edip, istediğiniz programlama dilinde kodlayın. Şifreleme işlemi yapacak fonksiyonunuz bu işlem için tek alfabe kullanacaktır.

Şifrele_deşifreleme_alfabe(açık_metin, alfabe, mod= (şifrele, deşifrele)) → şifreli_metin

Alfabe ve açık metini parametre olarak alan ve açık metini verilen alfabeye uygun olarak şifreli metin üreten bir fonksiyon dizayn edip, istediğiniz programlama dilinde kodlayın.

B. Uygulamanın Yapılışı:

a) Tasarladığınız fonksiyonu önce tek alfabeli, daha sonra çok alfabeli şifreleme yöntemi kullanarak büyük ve boyutlu verilerin şifrelenmesinde kullanınız.

Şifreleme / deşifreleme tasarımıza mesajla sahipleri tarafından bilinebilecek gizli anahtar değeri ekleyerek aşağıdaki şekilde tekrar düzenleyip örnek verilerin şifrelenmesinde kullanınız ve sonuçları değerlendirin.

Şifreleme_deşifreleme (açık_metin, gizli_anahtar, mod= (şifrele, deşifrele)) → şifreli_metin

b) Şifrele_deşifreleme_alfabe(açık_metin, alfabe, mod= (şifrele, deşifrele)) → şifreli_metin fonksiyonunuza alfabe olarak Tabloda tanımlanmış morse alfabesi vererek herhangi bir açık metni morse alfabesine dönüştüren veya morse alfabesinde kodlanmış bir metni açık metne geri dönüştürün.

Tablo 1 Mors Alfabesi Harf Kod Tablosu

Harf	Kod	Karakter	Kod
Aa	·−	.	·−·−·−
Bb	−···	,	−−··−−
Cc	−·−·	?	··−−··
Çç	−·−··	,	·−−−−·
Dd	−··	!	−·−·−−
Ee	·	/	−··−·
Ff	··−·	(	−·−−·
Gg	−−·	)	−·−−·−
Ğğ	−−·−·	:	−−−···
Hh	····	;	−·−·−·
Ii	··	=	−···−
Jj	·−−−	+	·−·−·
Kk	−·−	-	−····−
Ll	·−··	_	··−−·−
Mm	−−	“	·−··−·
Nn	−·	@	·−−·−·
Oo	−−−	Error	········
Öö	−−−·		
Pp	·−−·	Sayılar	
Qq	−−·−	Sayı	Kod
Rr	·−·	0	−−−−−
Ss	···	1	·−−−−
Tt	−	2	··−−−
Uu	··−	3	···−−
Üü	··−−	4	····−
Vv	···−	5	·····
Ww	·−−	6	−····
Xx	−··−	7	−−···
Yy	−·−−	8	−−−··
Zz	−−··	9	−−−−·

c) Size verilen morse alfabesine ait ses dosyalarını kullanarak verilen açık metni morse alfabesine uygun ses çıktısına dönüştüren programı kodlayın.

ANALİZ :

- Tasarladığınız fonksiyonları açıklayın, diğer tasarımlara göre güçlü ve zayıf yönlerini sıralayın.
- Gizli anahtarın boyutunun tasarladığınız sistem üzerindeki etkisi gözleyin ve gözlemlerinizi sıralayın.

REFERANSLAR :

1 – Morse Alfabesi, https://en.wikipedia.org/wiki/Morse_code, Son erişim tarihi : 20.11.2015

2- Morse Alfabesi Ses Kütüphanesi, https://en.wikipedia.org/wiki/Morse_code, Son erişim tarihi : 20.11.2015