**Bilgi Güvenliği ve Kriptoloji**

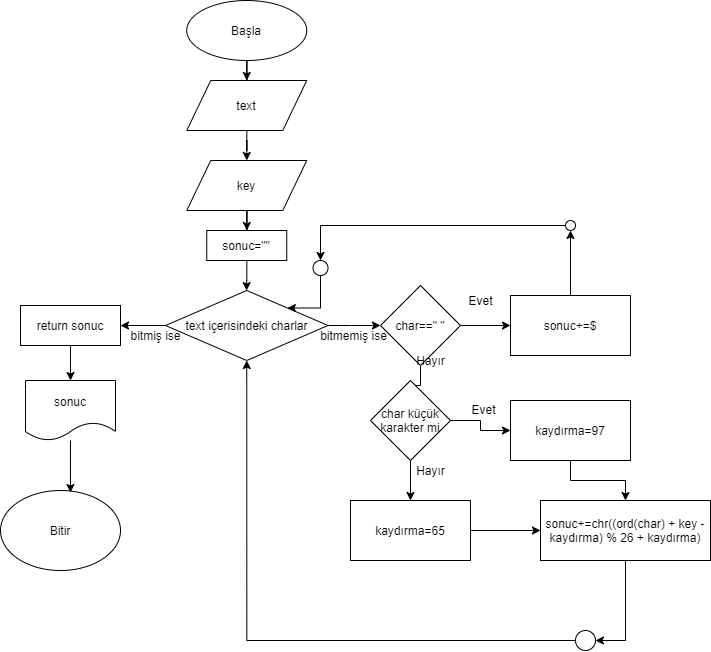
**Şifreleme algoritmaları rapor.**

**Sezar Algoritması**

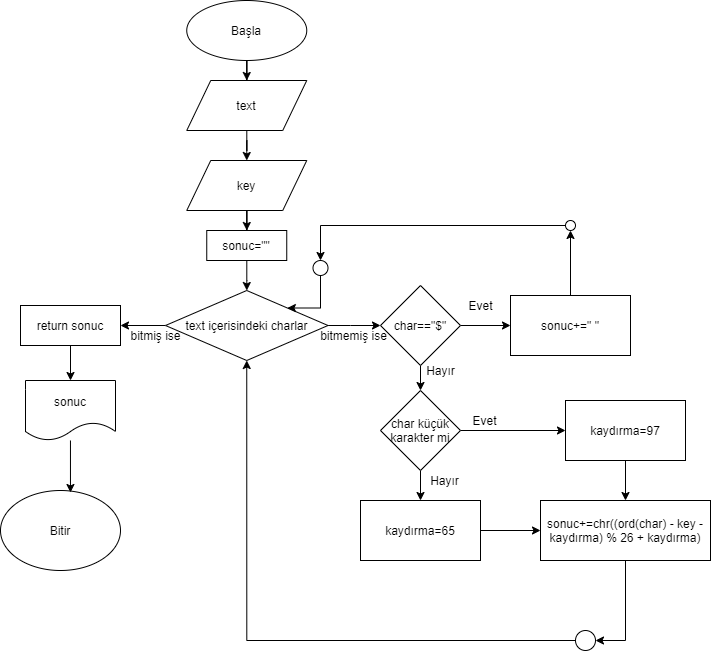
Sezar algoritması kullanıcının şifrelemek istediği metni alfabede kullanıcının belirlediği key kadar kaydırma işlemi yapılarak şifreli metin elde etme şeklinde gerçekleşir.

Benim kodladığım sezar algoritmasında kullanıcının girdiği metin char char gezilerek büyük veya küçük olması durumuna göre ascii kodlarında key kadar kaydırma işlemi yapar ve ufak bir hesaplama ile eğer key sonucu alfebenin sonuna gelinirse alfabenin başına dönülmesi sağlanmıştır. Ayrıca işlemleri ascii karakterler ile sağladığım için boşluk karakteri şifreyi çözme konusunda sıkıntı çıkartıyordu bunun önüne boşluk gördüğüm zaman onları $ şeklinde şifreleyerek geçmeye çalıştım.

**Sezar Şifreleme algoritmasının akış diyagramı**

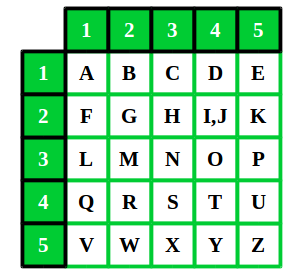


**Sezar algoritması ile şifrelenmiş bir metnin şifresinin çözülmesi akış diyagramı**



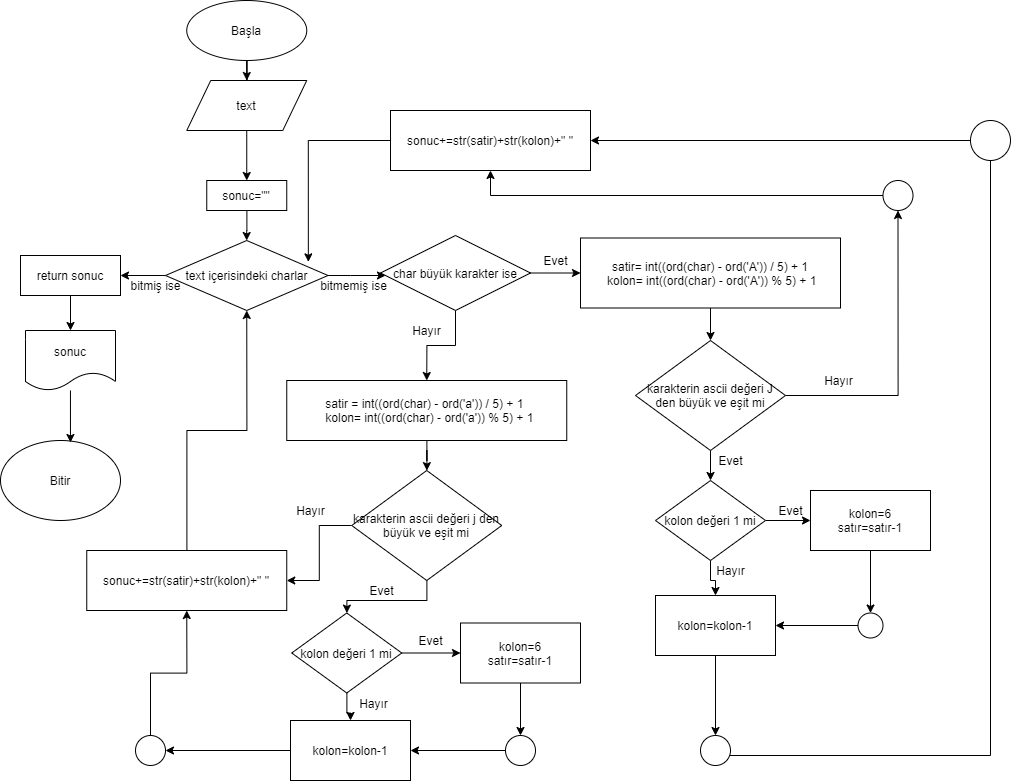
**Polybius şifreleme**

Kullanıcının girdiği metni kullanıcının alfabeyi 5x5 lik bir matrise bölerek metindeki ilgili charların satır ve sütun bilgisini geri döndüren bir şifreleme algoritmasıdır.



Uyguladığım algoritma da i ile j 2,4 e gelecek şekilde tasarladım. Ondan sonraki gelen charları birer birim kaydırarak işlemi tamamladım. Genel olarak girilen metini char char gezerek mevcut charın büyük ise 65 ile küçük ise 97 ile farkını alıp 5 e bölüp 1 ekleyerek satır değerini 5 e modunu alıp 1 ekleyerek ise sütün değerini buluyorum. İ ile j aynı değere sahip olduğu için j den sonraki bütün karakterlerde yapılan hesaplamalarda eğer kolon değerleri 1 çıkıyor ise onları 5. Kolona geri kaydırıyorum ve satır değerlerini 1 azaltıyorum mesela “K”

**Polybius şifreleme algoritmasının akış diyagramı**



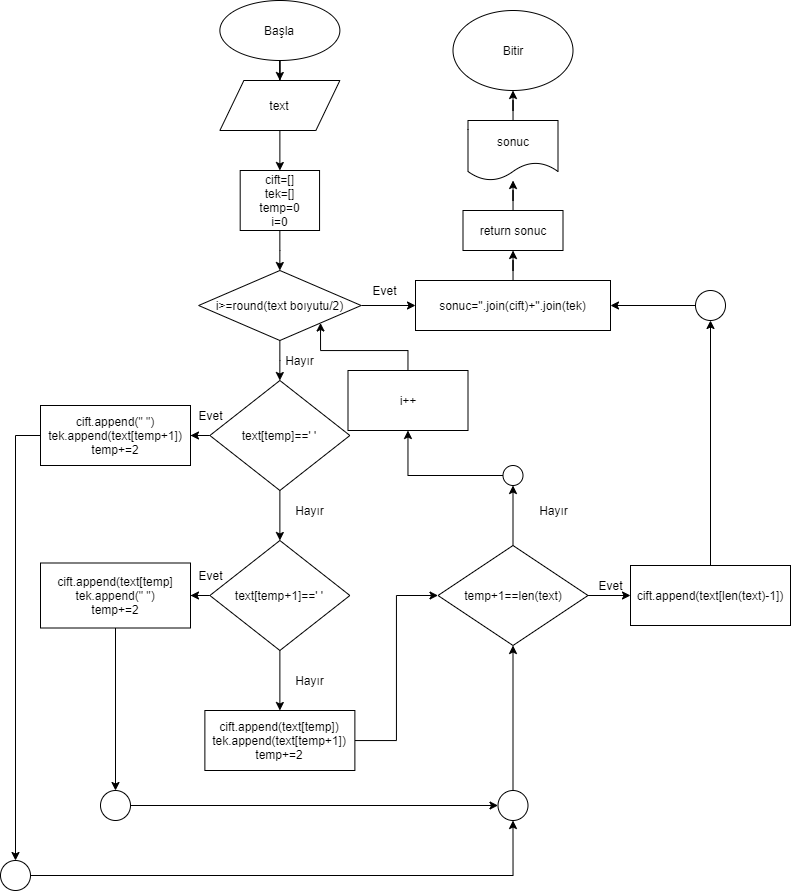
**Çit Şifreleme Algoritması**

Çit benzetmesi elimizdeki metni aynı bir çit üzerindeymiş gibi tek ve çift rakamlarına denk gelen bir şekilde 2 parçaya ayırıp bu iki parçayı birbirine bağlayarak yeni şifreli bir metin elde etmeye dayanır.

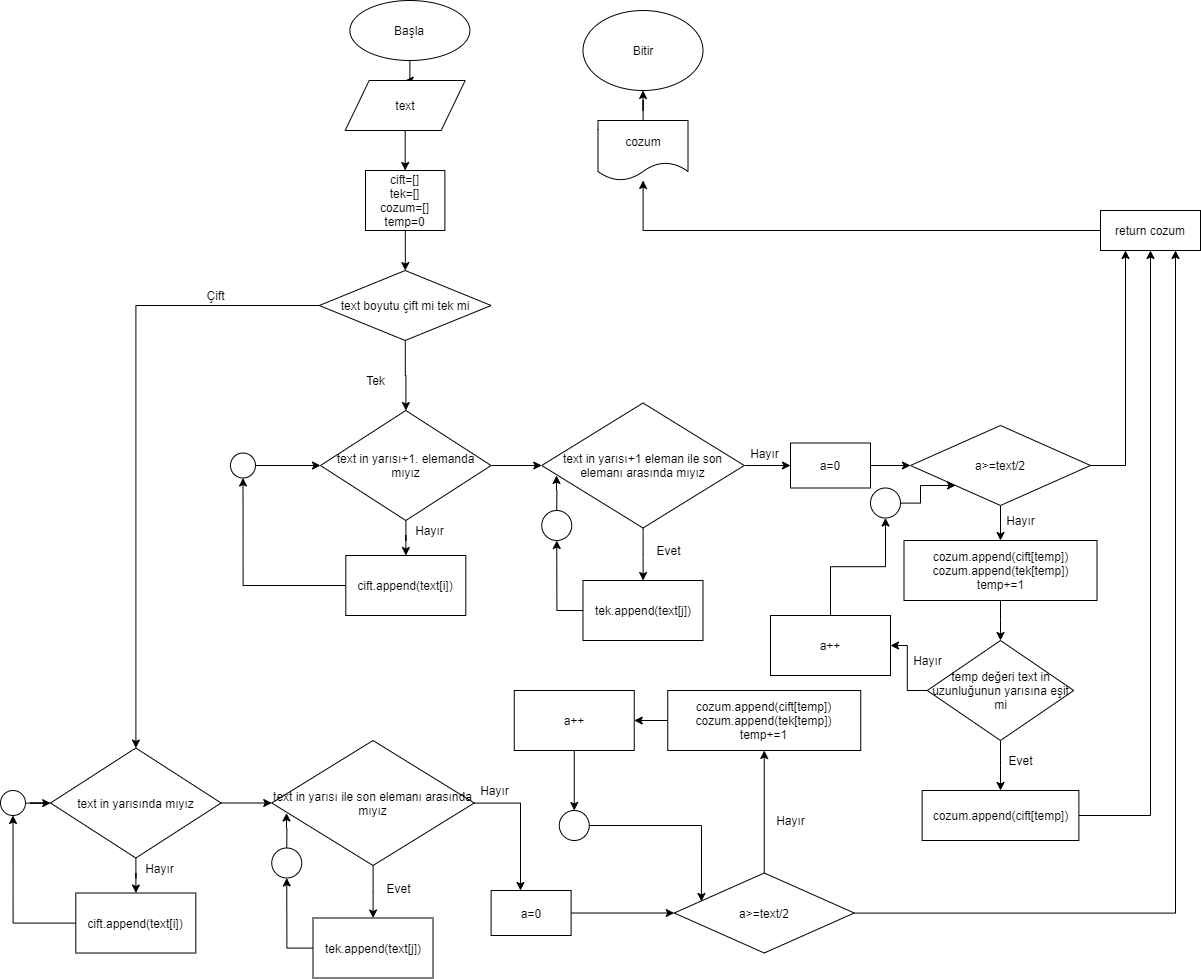
Kodlama yaparken elimdeki metni çift ve tek şeklinde oluşturduğum iki diziye karakter karakter atadım. Bunu yaparken o anki karakterin boşluk olup olmaması sorun çıkarttığı için buna uygun şekilde sıradaki karakterin boşluk olması veya bir sonraki karakterin boşluk olmasının kontrolünü sağlayıp ona uygun şekilde ikiye ayırma işlemi yaptım. Aynı şekilde girilen metnin uzunluğunun tek veya çift olmasına göre metni ikiye bölme işlemi yapıldığı zaman +1 karakter yani çift olan karakter dışarıda kalıyordu bunun içinde ayrı bir kontrol sağladım.

Aynı şekilde şifreleme yapılırken metin uzunluğunun tek ve çift olmasına göre iki farklı durum ve farklı çözme şekilleri vardır. Metin tek uzunlukta ise +1 karakter kalacaktır bu durum göz ardı edilmemelidir. Aynı şekilde elimizdeki şifreli metnin çift ve tek değerlerini for döngüsü ile dönerken metnin uzunluğu tek ise şifrelerken çift elemanlara +1 karakter verdiğimiz için çözerken de onu düşünmeliyiz. Ve farklı boyuttaki iki diziyi birbirine sırayla eklerken bu +1 karakterin kotrolünü uygun şekilde yapmalıyız.

**Çit şifreleme algoritmasının akış diyagramı**



**Çif şifre çözme algoritmasının akış diyagramı**



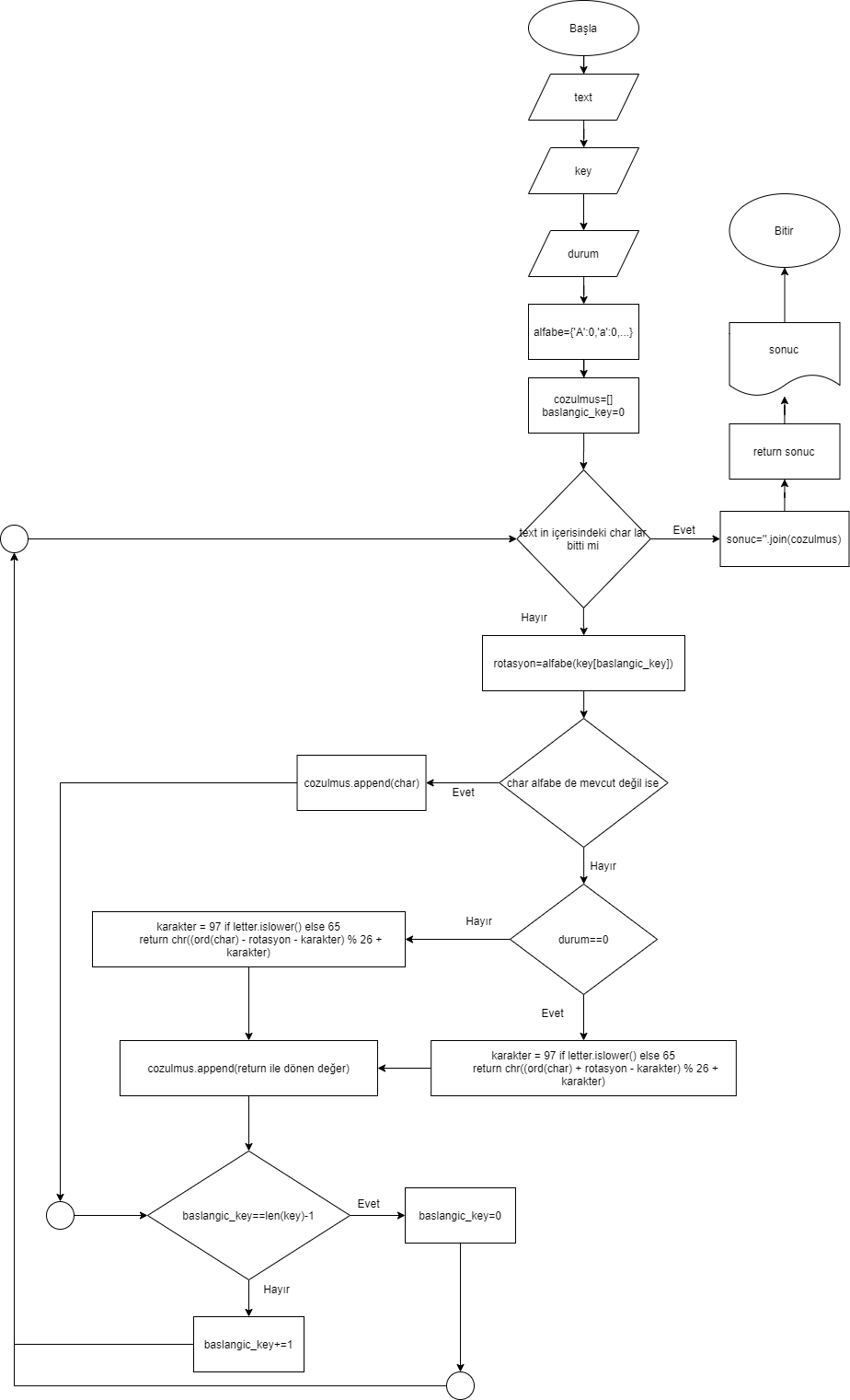
**Vinegere şifreleme algoritması**

Vinegere şifreleme metin ve şifre olarak text içerir basit şekilde metindeki charların sırasıyla şifredeki charların alfabedeki konumları kadar ileri kaydırılması ile şifrelenmiş metin elde edilir. Kodlama yaparken kendim alfabe ve bu alfabedeki karakterlerin konumlarına göre değerlerini tanımladım. Key ile metnin ilk karakterleri ile şifreleme işlemi başlıyor ve key son elemana geldiği zaman indexi sıfırlanıp key başa dönüyor. Böylece bütün metin key ile sıralı şekilde keyin o anki değerinin alfabedeki konumu kadar kaydırılıyor.

Şifre çözme adımında ise kaydırma işlemi yani sezar algoritması ters şekilde çalışıyor ve şifre çözülmüş olunuyor.

Şifreleme ve çözme için bir durum değişkeni tanımladım. Durum 0 ise şifreleme(ileri yönlü sezar) 1 ise şifre çözme(ters yönlü sezar) işlemi yaptırıyorum.

**Vinegere algoritması şifreleme ve şifre çözme akış diyagramı**



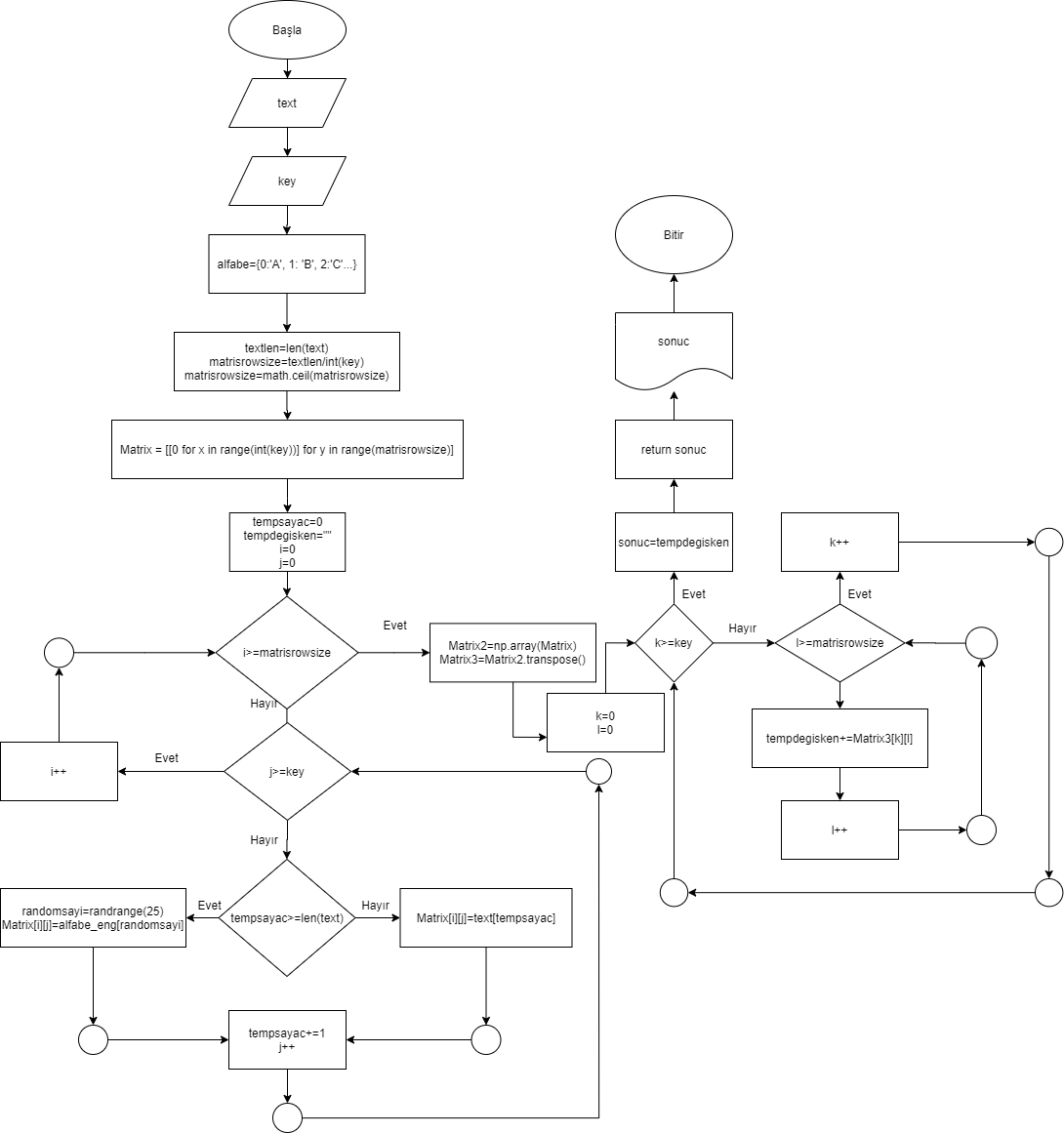
**Kolon Şifreleme Algoritması**

Kullanıcıdan metin ve key olarak bir rakam alınır. Alınan metin key kadar kolona sahip uygun bir matrise yerleştirilir ve bu matriste boşta kalan yerleşe alfabeden rastgele harfler eklenir. Daha sonra oluşan matris yukarıdan aşşağıya kolonlarca birbiri ardına eklenerek şifreli metni oluşturur.

Kodlama yaparken matrisin key i istenilen kolon sayısını oluşturuyor sayır sayısını ise alınan text in uzunluğunu key e bölerek elde ettim. Bütün elemanları 0 dan oluşan uygun 2 boyutlu matrisi oluşturdum ve iç içe forlar ile elimdeki text i matrise tanımladım. Eğer ki yapılan iş sayısı textin eleman sayısından büyük olmuş ise bu matris de boşta elemanlar var demek ve bunu alfabemdeki eleman sayısı kadar bir aralıkta random sayı üretip boşlukları oradan dönen harfler ile doldurarak çözdüm. Daha sonra mevcut matrisin transpozunu alıp yazdırdım ve şifrelenmiş text i elde etmiş oldum.

Şifrelenmiş metnin çözümü kısmında aynı şekilde key doğrultusunda uygun matrise metni yerleştirdim ve transpozun transpozu tekrar metnin kendisine eşit olacağından oluşan matrisin transpozunu alıp yazdırdım ve şifreli metnin şifresi çözülmüş oldu.

**Kolon algoritması şifreleme akış diyagramı**



**Kolon algoritması şifreli metin çözme algoritması akış diyagramı**

