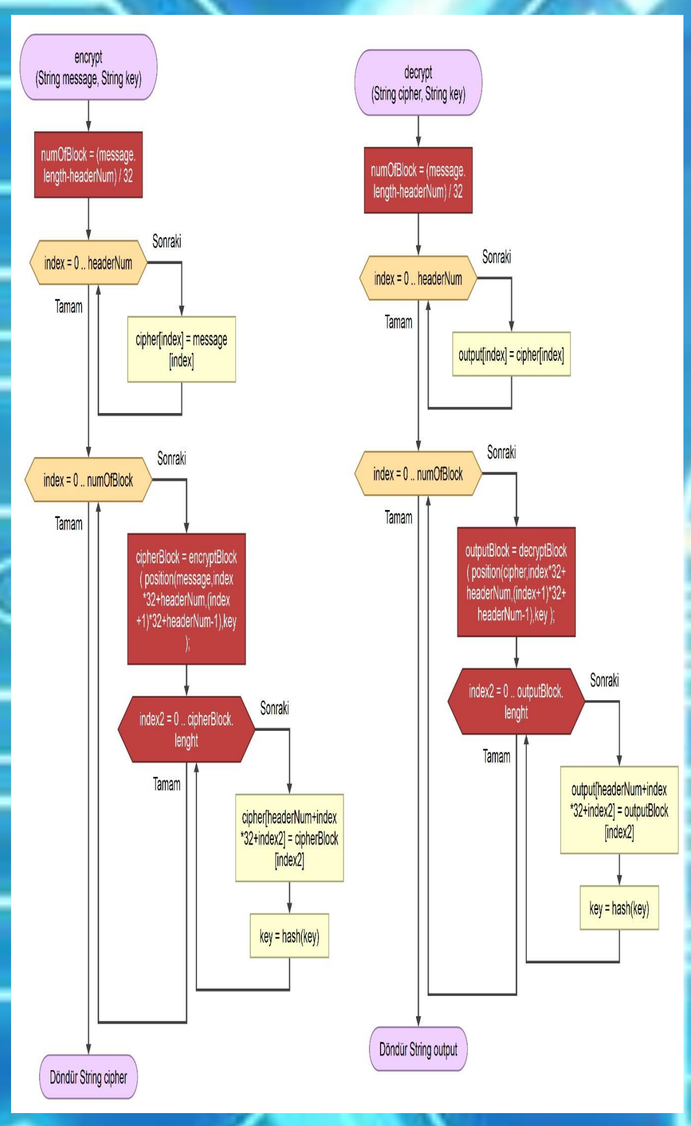
VERİ GÜVENLİĞİ

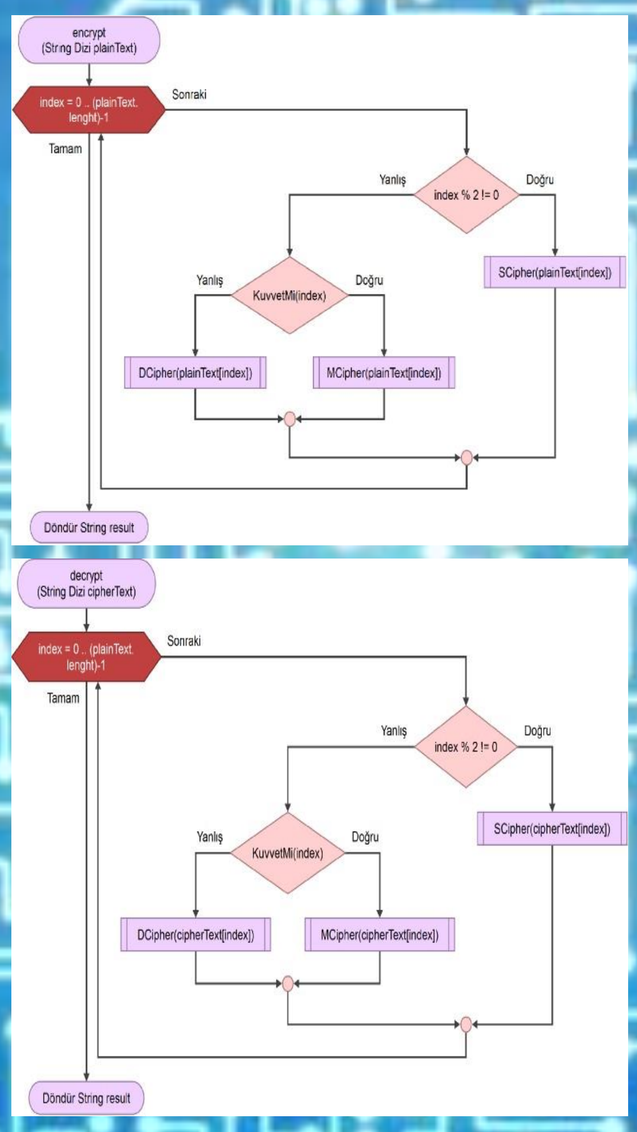
Onur BUDAK
Batuhan EKİCİ
Hakan AKSOY

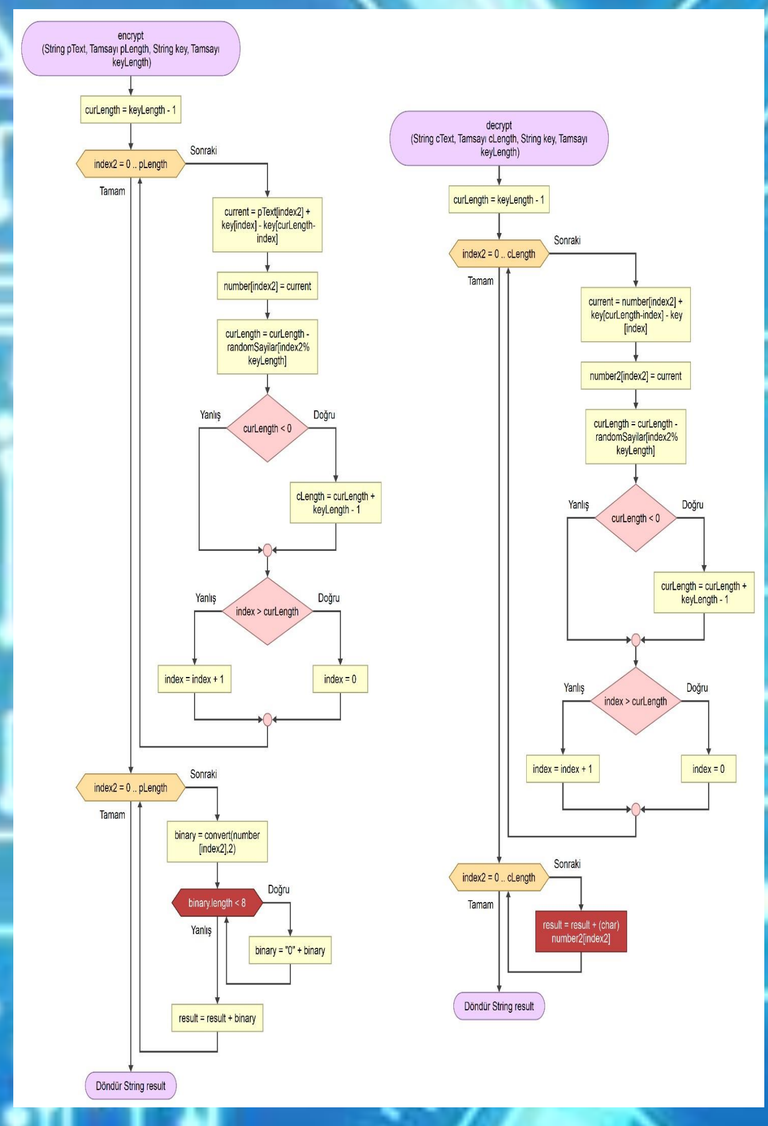
Danışman
Doç. Dr. Güzin ULUTAŞ

GİRİŞ

Günümüzde güvenli iletişim için veri gönderiminin önemi oldukça fazladır. Bu amaçla var olan şifreleme tekniklerinden de yola çıkarak şifreleme algoritmaları tasarlanmıştır. Verinin şifrelenmesi aşamasında gizli anahtar ve tablo mevcuttur. Şifreleme algoritmalarının her birinde farklı teknikler kullanılmıştır ve bu yüzden her birinin brute-force (kaba-kuvvet) testine karşı dayanıklılığı farklıdır.





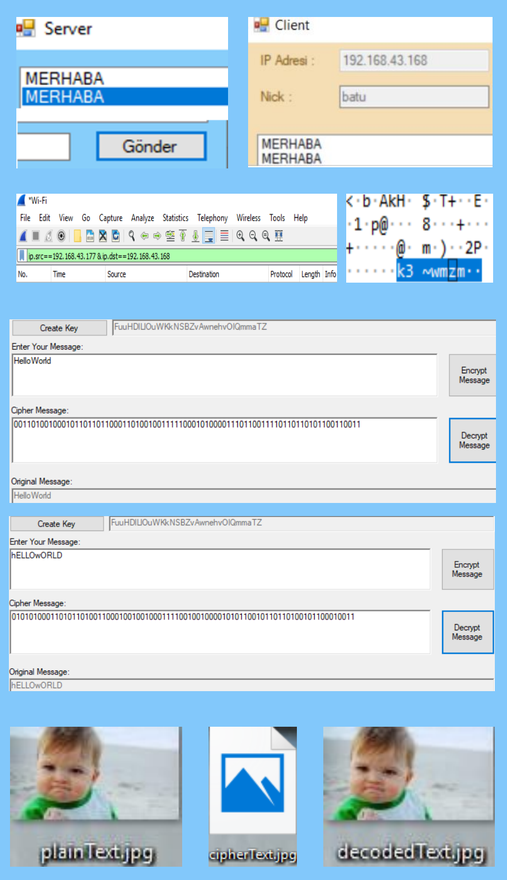


YÖNTEM

Tasarlanılan şifreleme algoritmalarında şifreleme modlarından faydalanılmıştır. Bu modlar, şifreleme işlemine girecek olan açık metnin seçimi ve üzerinde gerçekleştirilebilecek işlemlerle ilgilidir.

Verinin şifrelenmesi için kullanılan simetrik ve asimetrik yöntemler SSL (Secure Socket Layer) yapısında kullanılır. Simetrik yapı; şifreleme ve şifre çözmenin daha önceden paylaşılmış bir anahtar ile yapıldığı şifreleme mevcuttur. Asimetrikte yapıda ise; şifreleme ve deşifreleme işlemi için ayrı anahtar kullanılmaktadır.

UYGULAMA



SONUÇ

Şifreleme algoritmalarının testlerinde kullanılabilecek sunucu-istemci mimarisi SSL'in güvenlik standartını içermesi gerekmektedir.

Algoritma tasarım işlemi tamamlandıktan sonra SSL protokolünde mevcut olan; Handshake, Alert ve Record protokollerini içeren bir implementasyonu sağlama işlemine geçiş yapılacaktır.