

VERİ GÜVENLİĞİ

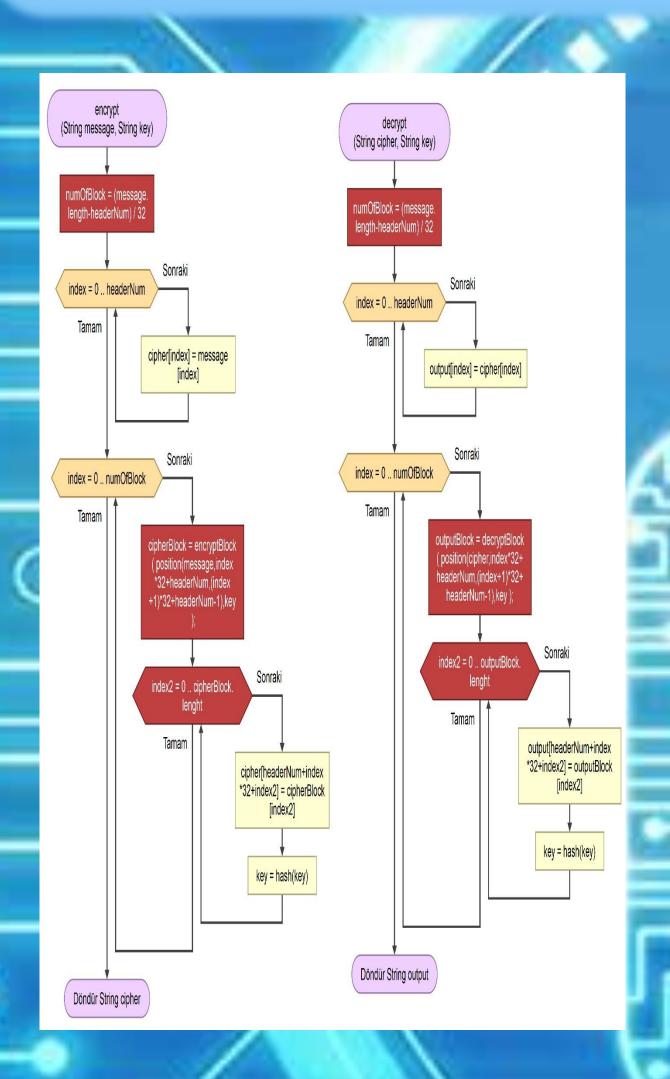
Onur BUDAK Batuhan EKİCİ Hakan AKSOY

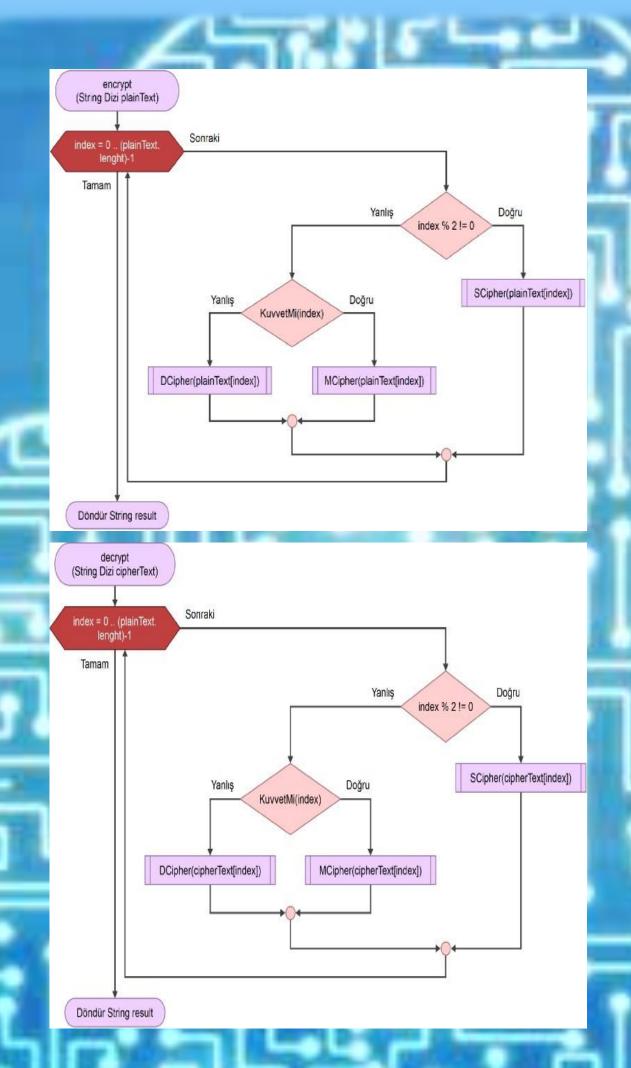


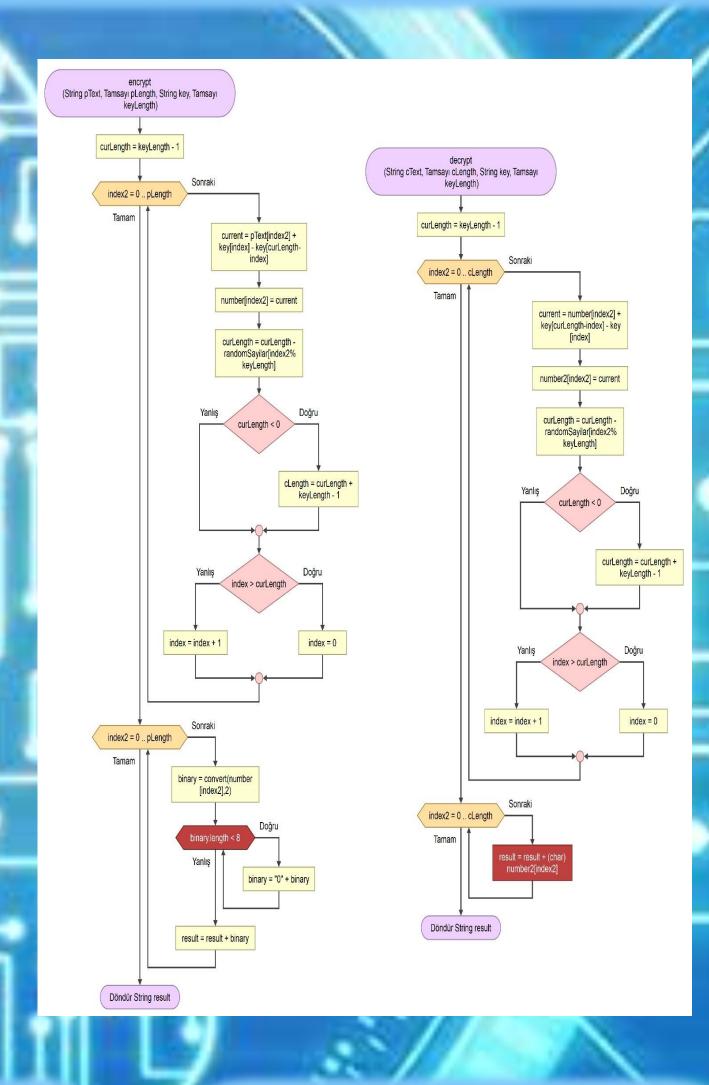


GİRİŞ

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

IP Adresi: 192.168.43.168 Nick: batu MERHABA MERHABA MERHABA Nick: batu MERHABA MERHABA MERHABA Nick: batu MERHABA MERHABA MERHABA Nick: batu MERHABA MERHABA Nick: batu MERHABA MERHABA Nick: batu MERHABA Nick: batu MERHABA Nick: batu Message 190.168.43.168 Nick: batu Message Nick: batu Message Nick: batu Message Nick: batu Message Nick: batu Message Nick: batu Decrypt Message Message Decrypt Message Decrypt Message	🖳 Server		Client		
MERHABA MER				T	_
MERHABA Merender Merend	MEDITARA		IP Adresi:	192.168.43.16	8
MERHABA Merender Merend	MERHABA MERHABA		Minds .	In order	
MERHABA Malyze Statistics Telephony Wireless Tools Help	MERHABA		NICK :	Datu	
MERHABA Malyze Statistics Telephony Wireless Tools Help					
Inalyze Statistics Telephony Wireless Tools Help Separation Protocol Length Info Destination Protocol Length Info Destination Protocol Length Info Destination Protocol Length Info Decorpt Length Info Decorpt Length Info	Gönd	ler			
Destination			MERHABA		
168,43,168	✓ *Wi-Fi			Z . b . A k H .	₹. T⊥ E.
168,43,168		Statistics Telephony Wire	less Tools Help	A -O	⊅.1 ±Ε.
168.43.168 Destination Protocol Length Info R3				.1.b@	8+
Encrypt	ip.src==192.168.43.177 & ip.dst==192.168.43.			+ · · · · · · @ ·	m·)2P·
Encrypt Message	No. Time Source		Protocol Length Info	k3	~wmzm··
Encrypt Message					
Encrypt Message					
Message	Create Key FuuHDILIOuV	VKkNSBZvAwnehvOlQmn	naTZ		
Message	nter Your Message:				
10010011111100010100001110110111101110	Hello World				
Decrypt Message LIOuWKkNSBZvAwnehvOlQmmaTZ Encrypt Message 00100011110010010000101101101101101101					Message
Decrypt Message LIOuWKkNSBZvAwnehvOlQmmaTZ Encrypt Message 00100011110010010000101101101101101101	ipher Message:				
Message	0011010010001011011011011000110100100	011111000101000011101	10011110110110101100	110011	Doorunt
Encrypt Message 00100011110010010000101101101101101101					
Encrypt Message 00100011110010010000101101101101101101					
Encrypt Message 00100011110010010000101101101101101101					
Encrypt Message 0010001111001001000010110110110110110101					
001000111100100100001010110010110110110					
001000111100100100001010110010110110110	HelloWorld	KkNSBZvAwnehvOlQmma	nTZ		
001000111100100100001010110010110110110	HelloWorld Create Key FuuHDILIOuW inter Your Message:	Kk NSBZv Awnehv OlQmma	яTZ		
Decrypt	HelloWorld Create Key FuuHDILIOuW	Kk NSBZvAwnehvOlQmma	лZ		
Decrypt	HelloWorld Create Key FuuHDILIOuW	Kk,NSBZvAwnehvOlQmma	īΤΖ		
	HelloWorld Create Key FuuHDILIOuW inter Your Message: ELLOwORLD	Kk NSBZv Awnehv OlQmma	iTZ		
	HelloWorld Create Key FuuHDILIOuW inter Your Message: hELLOwORLD ipher Message:			0011	Message
	HelloWorld Create Key FuuHDILIOuW inter Your Message: hELLOwORLD ipher Message:			0011	Message
	Create Key FuuHDILIOuW nter Your Message: ELLOwORLD ipher Message:			0011	Message
	HelloWorld Create Key FuuHDILIOuW inter Your Message: nELLOwORLD ipher Message: 010101000110101101001100010010010010010			0011	Message
	Original Message:	KkNSBZvAwnehvOlQmma	nTZ		
	Create Key FuuHDILIOuW Your Message: OwORLD r Message: 01000110101101001100010010010000000000			0011	Message
	Create Key FuuHDILIOuW tter Your Message: ELLOWORLD oher Message: 101010001101011010010010010010010010010			0011	Message
	Create Key FuuHDILIOuW nter Your Message: ELLOWORLD pher Message: 101010001101011010011000100100100100100			0011	Message
	Create Key FuuHDILIOuW nter Your Message: ELLOwORLD pher Message: 101010001101011010011000100100100100100			0011	Message
	HelloWorld Create Key FuuHDILIOuW Inter Your Message: IELLOWORLD Ipher Message: I101010001101011010011000100100100100100			0011	Message
	HelloWorld Create Key FuuHDILIOuW inter Your Message: hELLOwORLD iipher Message: 110101000110101101001100010010010010010			0011	Message
	HelloWorld Create Key FuuHDILIOuW inter Your Message: hELLOwORLD ipher Message: 110101000110101101001100010010010010010			0011	Message
	Create Key FuuHDILIOuW nter Your Message: ELLOwORLD pher Message: 101010001101011010011000100100100100100			0011	Message
g cipherText.jpg decodedText.jpg	HelloWorld Create Key FuuHDILIOuW Inter Your Message: IELLOWORLD Ipher Message: I101010001101011010011000100100100100100	0111100100100001010110	00101101101001011000		Decrypt Message

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.