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 yola çıkarak şifreleme algoritmaları tasarlanmıştır. Verinin şifrelenmesi aşamasında gizli anahtar ve tablo kullanılmıştır. Şifreleme algoritmalarının her birinde farklı teknikler kullanılmıştır ve bu sebeple her birinin brute-force (kaba-kuvvet) testine karşı dayanıklılığı farklıdır.

PLAYFAİR MATRİSİ

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y

Konum = Giriş[i] + key [j] – key [boy – j]
Konum2 = Şifreli[i] + key [boy – j] – key [j]

C1 = P1 ⊕ Key ⊕ H(Key)
Key2 = H(Key)
C2 = P2 ⊕ Key2 ⊕ H(Key2)
Key3 = H(Key2)
...
Cn = Pn ⊕ Keyn ⊕ H(Keyn)

P1 = C1 ⊕ Key ⊕ H(Key)
Key2 = H(Key)
P2 = C2 ⊕ Key2 ⊕ H(Key)
Key3 = H(Key2)
...
Pn = Cn ⊕ Key ⊕ H(Key)

KURALLAR

BİRİNCİ ADIM

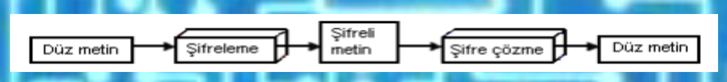
- Art arda gelen aynı karakterlerin arasına “X” eklenmesi
- Şifrelenecek metin eklenebilecek “X” karakteriyle birlikte tek sayıda karakter içeriyorsa, padding (doldurma) yapılarak karakter sayısı çifte tamamlanır.

İKİNCİ ADIM

- Parçalanan harf grupları eğer aynı satırda ise her harf için aynı satırda kendinden sonra gelen karakter (sağındaki eleman), aynı sütunda ise bir sonraki (aşağı) karakter seçilir.
- Belirtilen bu koşul dışında ise her harf için bulunduğu satır ve sütun kesişim noktalarındaki karakter baz alınarak şifreleme işlemi yapılabilmektedir.

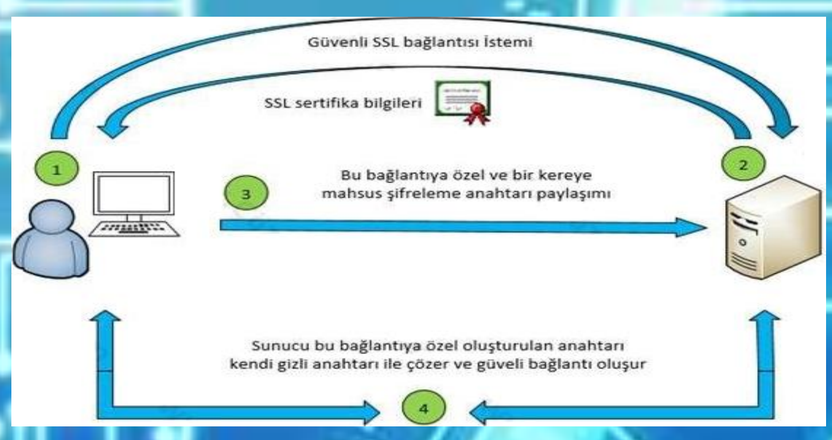
ANAHTAR BOYUTLARI

Simetrik Şifreleme – 1 : **2^256**
Simetrik Şifreleme – 2 : **2^182**
Simetrik Şifreleme – 3 : **Tablo**



ŞİFRELENECEK VERİ: TABLETENNIS

PLAİN TEXT	CİPHER TEXT
TA-BL-ET-EN-NI-SX	EPGQJYODSNXD
EP-GQ-JY-OD-SN-XD	TALVOEENXSDI
TA-LV-OE-EN-XS-DI	EPQBTJODDXIN
EP-QB-TJ-OD-DX-IN	TAVGYOENIDNS
TA-VG-YO-EN-ID-NS	EPBLETODNISX

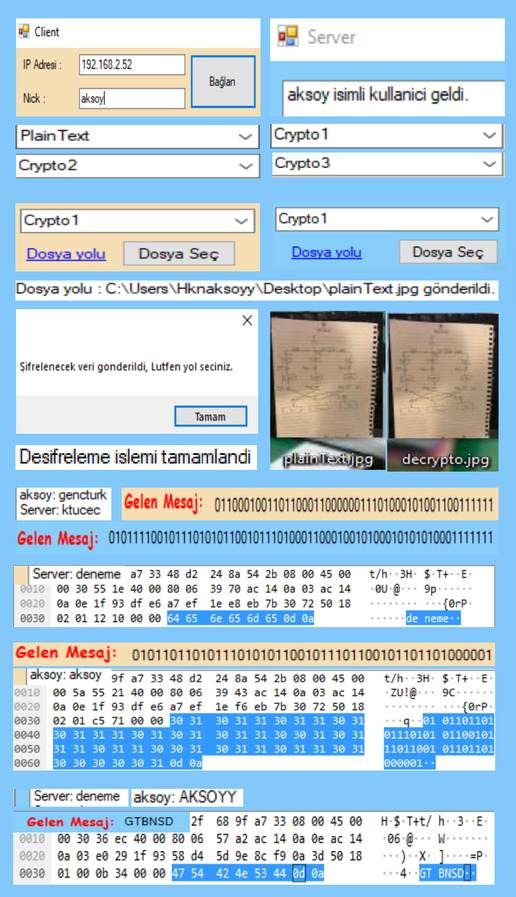


YÖNTEM

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

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 yapılmaktadır. Asimetrik 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.

Tasarlanılan simetrik şifreleme algoritmalarını içeren kütüphane yapısını kullanarak şifreleme ve deşifreleme işlemi güvenli şekilde yapılabilmektedir.