

Kriptoloji Dersi Proje Raporu

Client IP: 192.168.116.1

Server IP: 192.168.116.1

Client Port: 53439

Server Port: 53439

Analiz Aracı: Wireshark

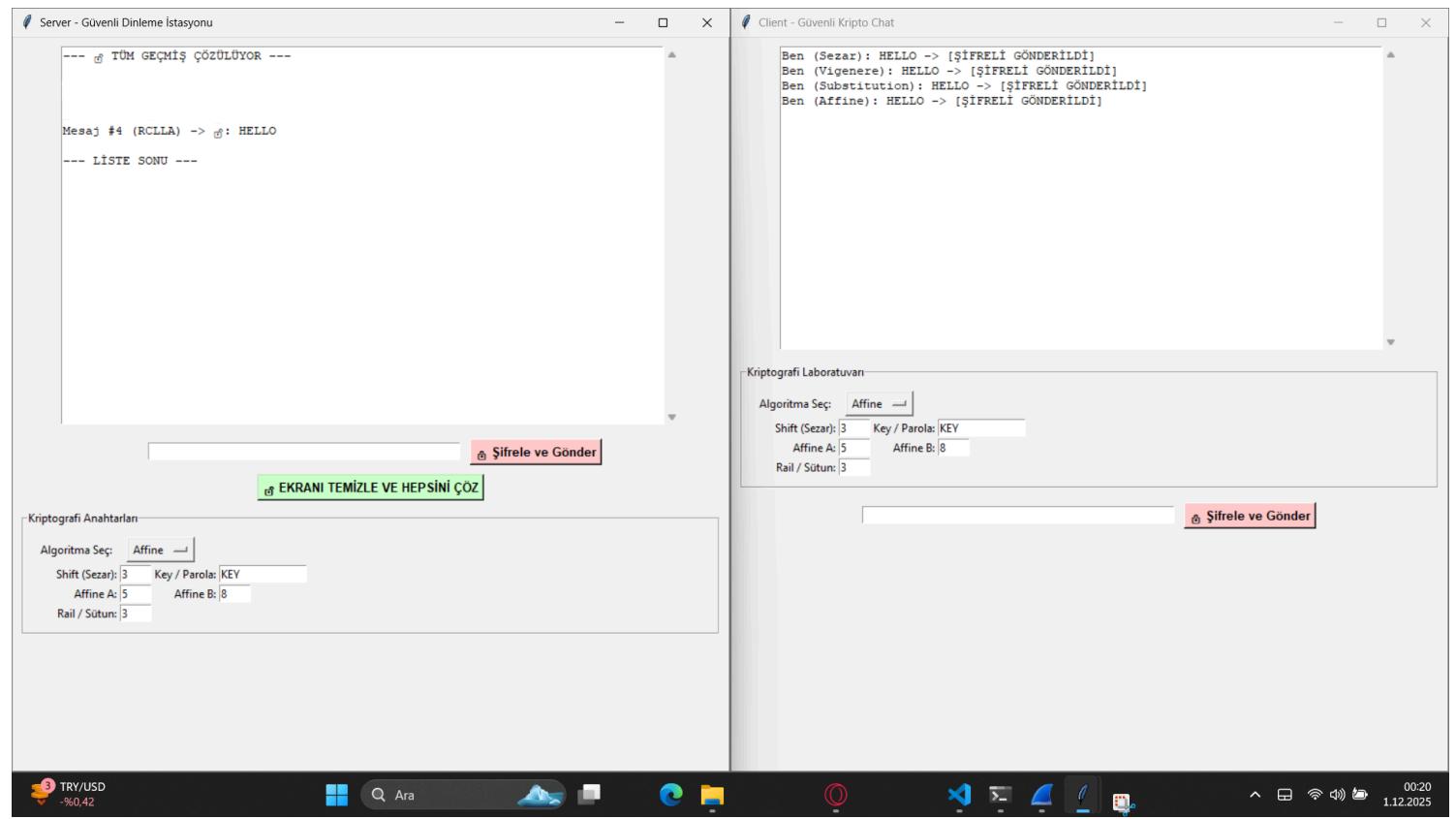
Protokol: TCP

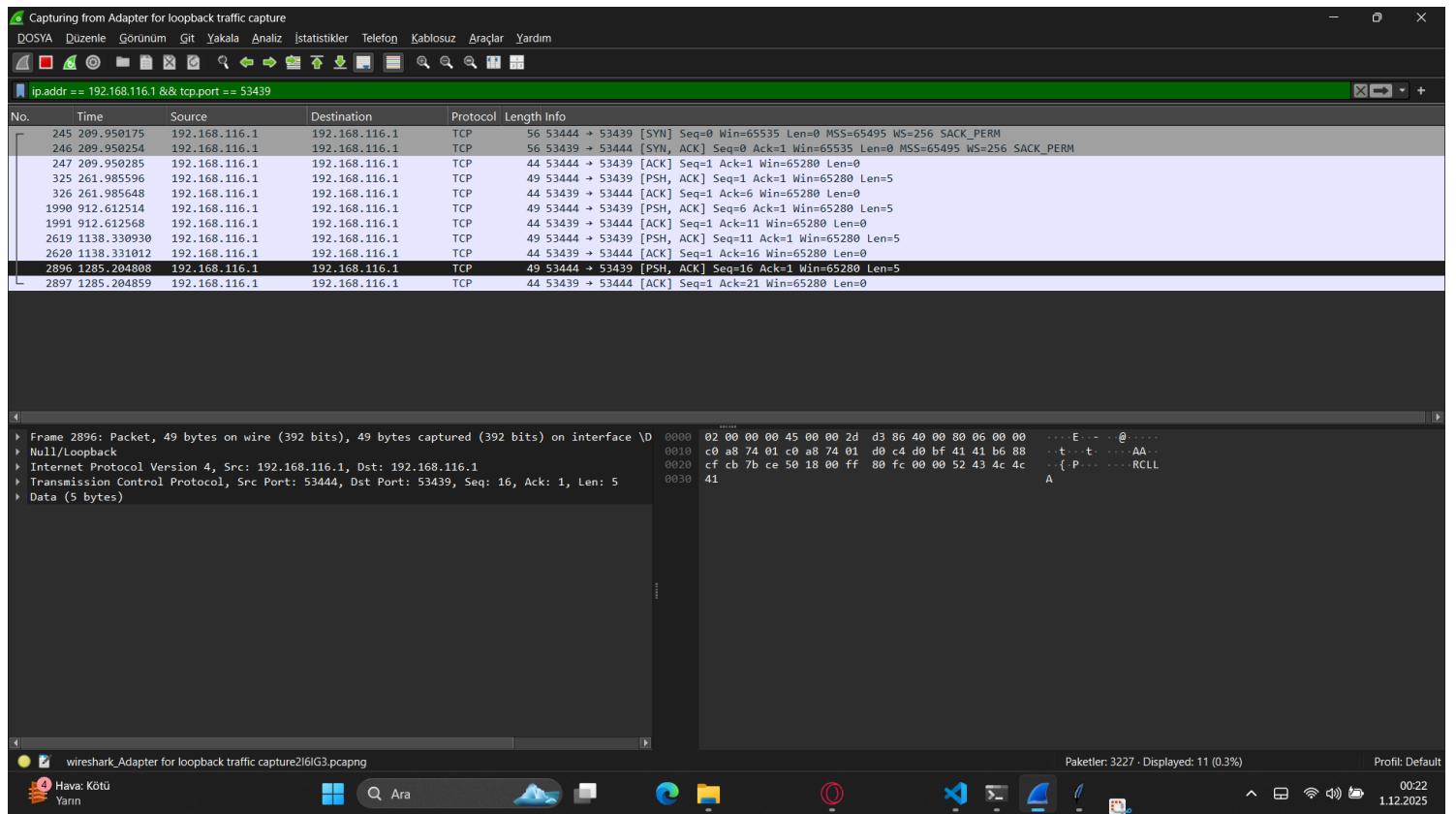
Tüm algoritmalar için aşağıdaki veri gönderilmiştir:

HELLO

Bu veri şifrelenmiş halleriyle analiz edilmiştir.

AFFINE CIPHER





Affine ile şifrelendiğinde Wireshark'ta karakterlerin dönüştüğü ama hâlâ okunabilir harflerden oluşan bir çıktı görünür. Yani mesaj plaintext değildir ama şifreli metin yine alfabeeye dayalıdır. Paket içeriği hala metin olarak okunabilir.

COLUMNAR CIPHER

Server - Güvenli Dinième İstasyonu

```
--- @ TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
Mesaj #8 (EOHLL_) -> @: HELLO
--- LİSTE SONU ---
```

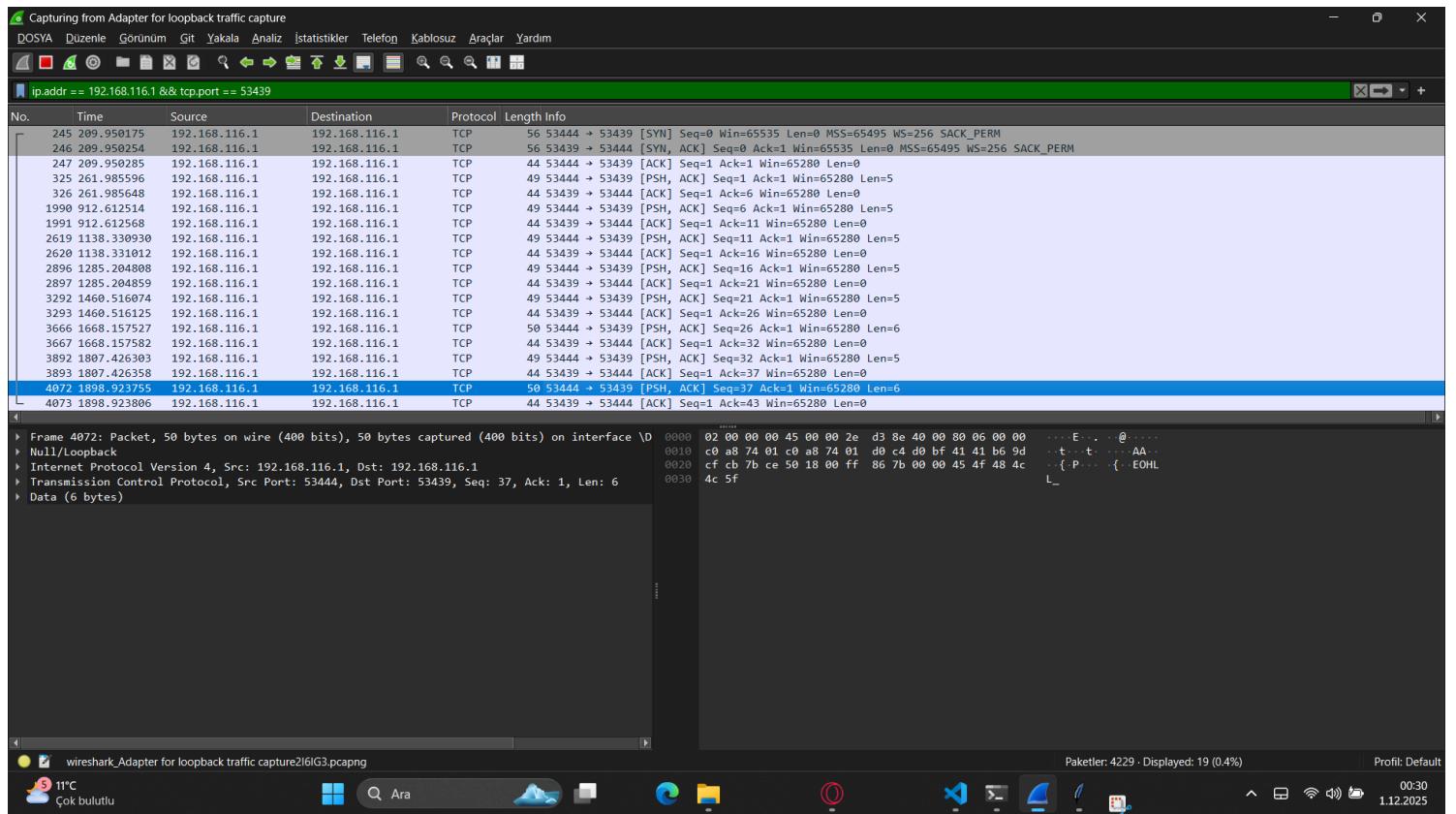
Client - Güvenli Kripto Chat

```
Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Columnar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
```

Kriptografi Laboratuvarı

Algoritma Seç: Columnar

Shift (Sezar): 3 Key / Parola: KEY
Affine A: 5 Affine B: 8
Rail / Sütun: 3



Columnar yöntemiyle şifrelenen HELLO mesajı Wireshark'ta harflerin yer değiştirilmiş hâliyle görünür. İçerik hala tamamen okunabilir ASCII harflerdenoluştugu için, Wireshark mesajı doğrudan gösterir.

DES CIPHER

Client (('192.168.116.1', 53444)) [GİZLİ]: 8959C9C9F9

Kriptografi Anahtarları

Algoritma Seç: DES —
 Shift (Sezar): 3 Key / Parola: KEY
 Affine A: 5 Affine B: 8
 Rail / Sütun: 3

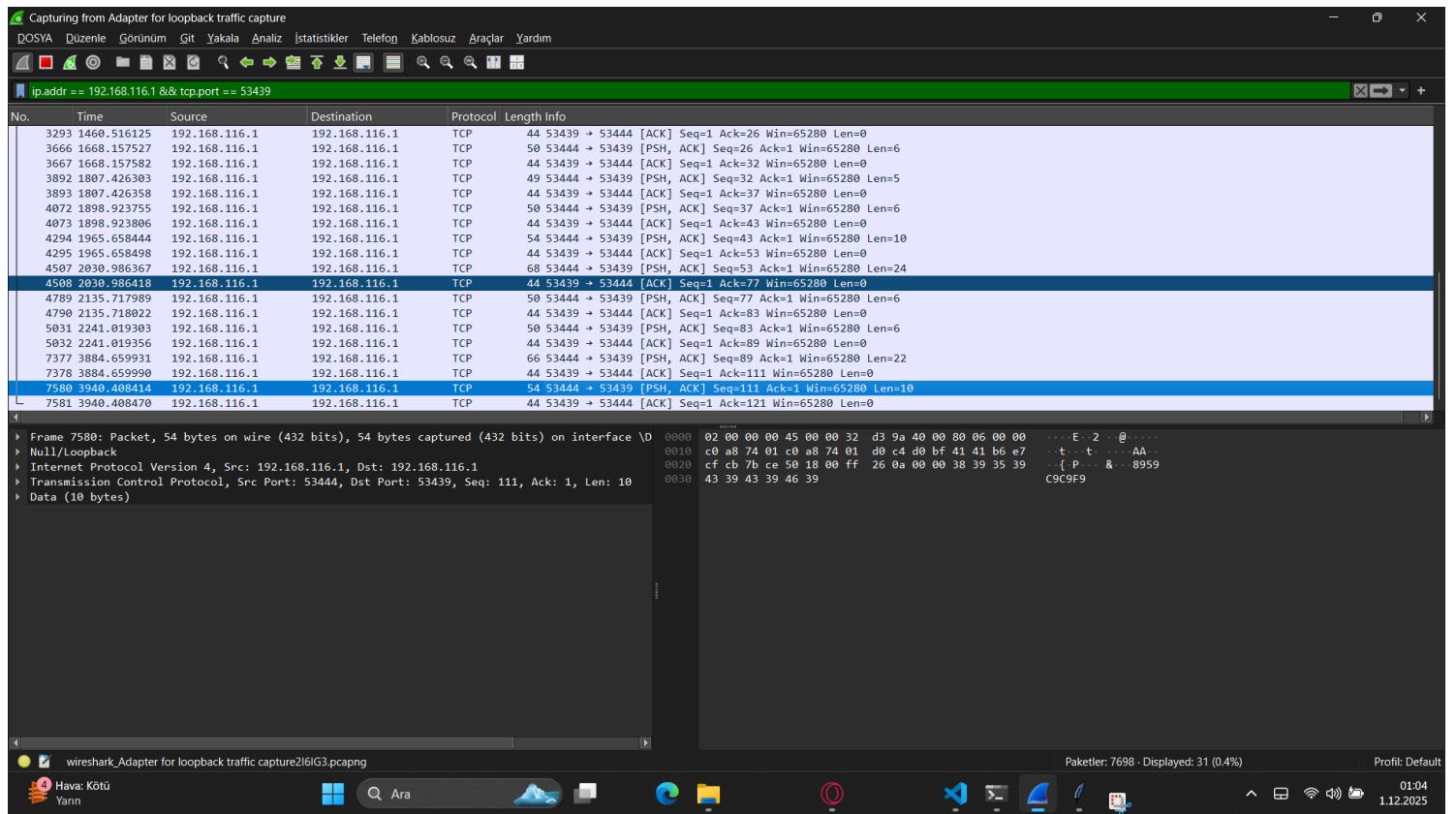
Kriptografi Laboratuvarı

Algoritma Seç: DES —
 Shift (Sezar): 3 Key / Parola: KEY
 Affine A: 5 Affine B: 8
 Rail / Sütun: 3

Şifrele ve Gönder

EKRANI TEMİZLE VE HEPŞİNİ ÇÖZ

Hava: Kötü Yann 01:04 11.2.2025



DES ile şifrelenen HELLO mesajı Wireshark'ta tamamen rastgele byte dizileri olarak görünür. Hiçbir şekilde okunabilir metin içermez. Orijinal mesaj çözülmmez.

DSA

Server - Güvenli Dinième İstasyonu

--- TÜM GEÇMİŞ ÇÖZÜLÜYOR ---

Mesaj #17 (HELLO|3,2) -> : HELLO (İmza Doğrulandı

--- LİSTE SONU ---

Kriptografi Anahtarları

Algoritma Seç: DSA

Shift (Sezar): 3 Key / Parola: KEY
Affine A: 5 Affine B: 8
Rail / Sütun: 3

Client - Güvenli Kripto Chat

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Columnar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Polybius): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Pigpen): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Route): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Hill): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (RSA): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (DES): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (DES): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (DES): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

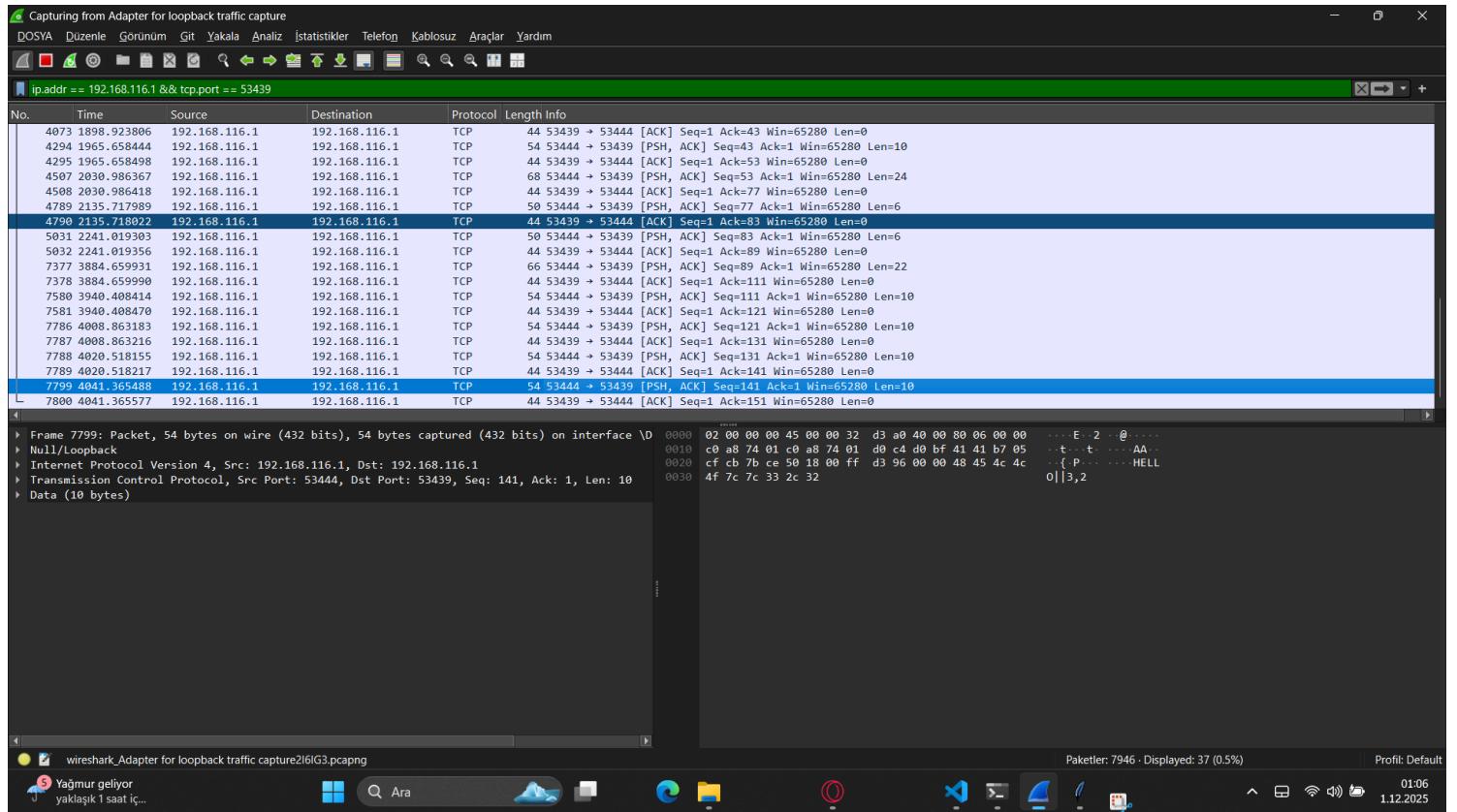
Kriptografi Laboratuvarı

Algoritma Seç: DSA

Shift (Sezar): 3 Key / Parola: KEY
Affine A: 5 Affine B: 8
Rail / Sütun: 3

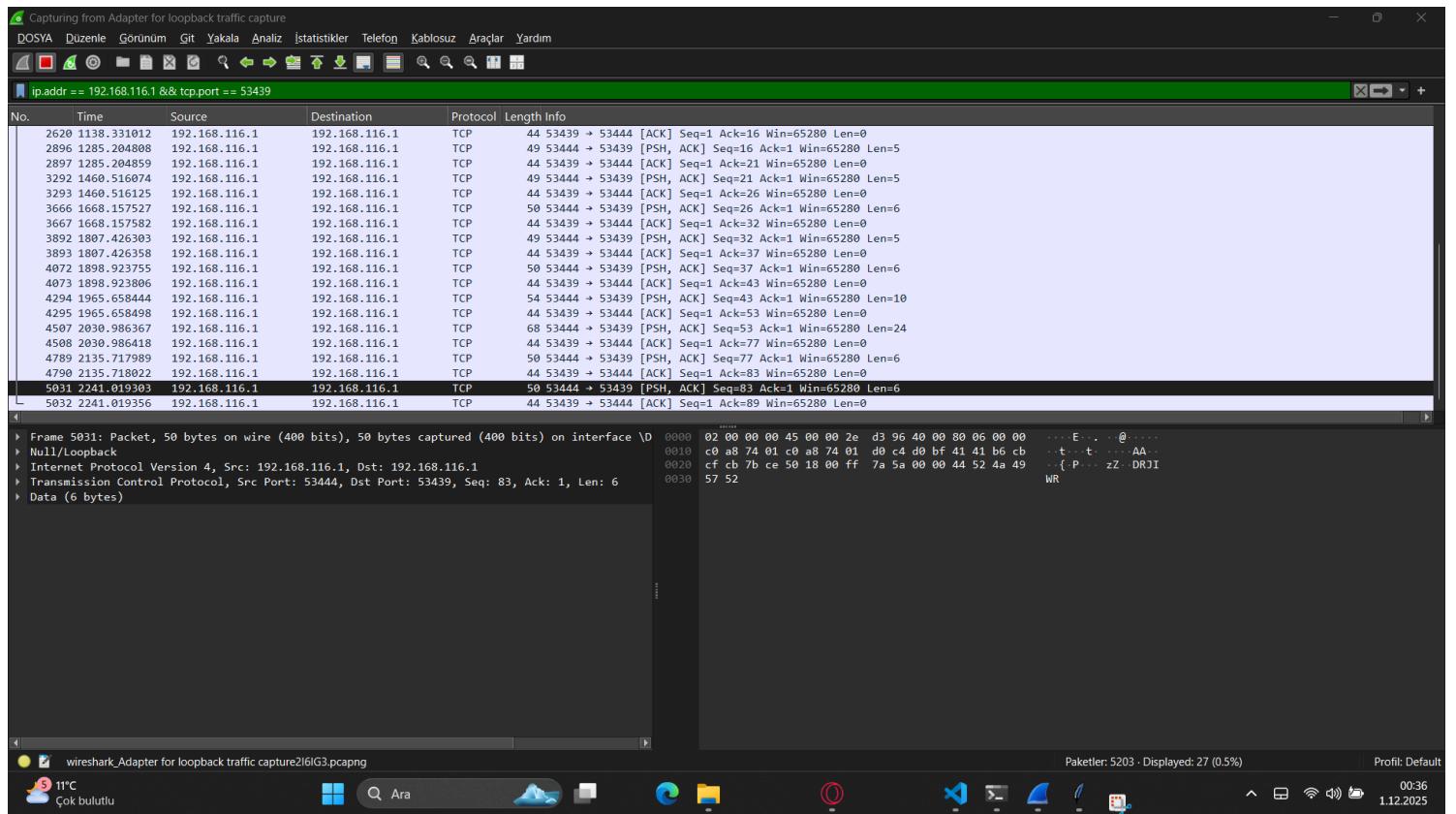
Hava: Kötü Yann

01:05 11.2.2025



DSA bir şifreleme algoritması olmadığı için HELLO mesajı Wireshark'ta okunabilir şekilde görünür. Ancak DSA tarafından üretilen imza verisi, Wireshark'ta rastgele byte'lardan oluşan bir imza bloğu şeklinde ortaya çıkar. Mesaj gizlenmez; sadece imzalanır.

HILL CIPHER



Hill cipher ile şifrelenen HELLO mesajı Wireshark'ta alfabetik, okunabilir ama karışık harflerden oluşan bir çıktı şeklinde görünür. Matris işlemleri sonucu harfler değişir fakat plaintext yapısı korunur.

PIGPEN CIPHER

Server - Güvenli Dinleme İstasyonu

TÜM GEÇMİŞ ÇÖZÜLÜYOR ---

Mesaj #10 (RCL *L *E*) -> : HELLO

--- LİSTE SONU ---

Şifrele ve Gönder

EKRANI TEMİZLE VE HEPİNİ ÇÖZ

Kriptografi Anahtarları

Algoritma Seç: Pigpen

Shift (Sezar): 3 Key / Parola: KEY

Affine A: 5 Affine B: 8

Rail / Sütun: 3

Client - Güvenli Kripto Chat

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Columnar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Polybius): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
 Ben (Pigpen): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

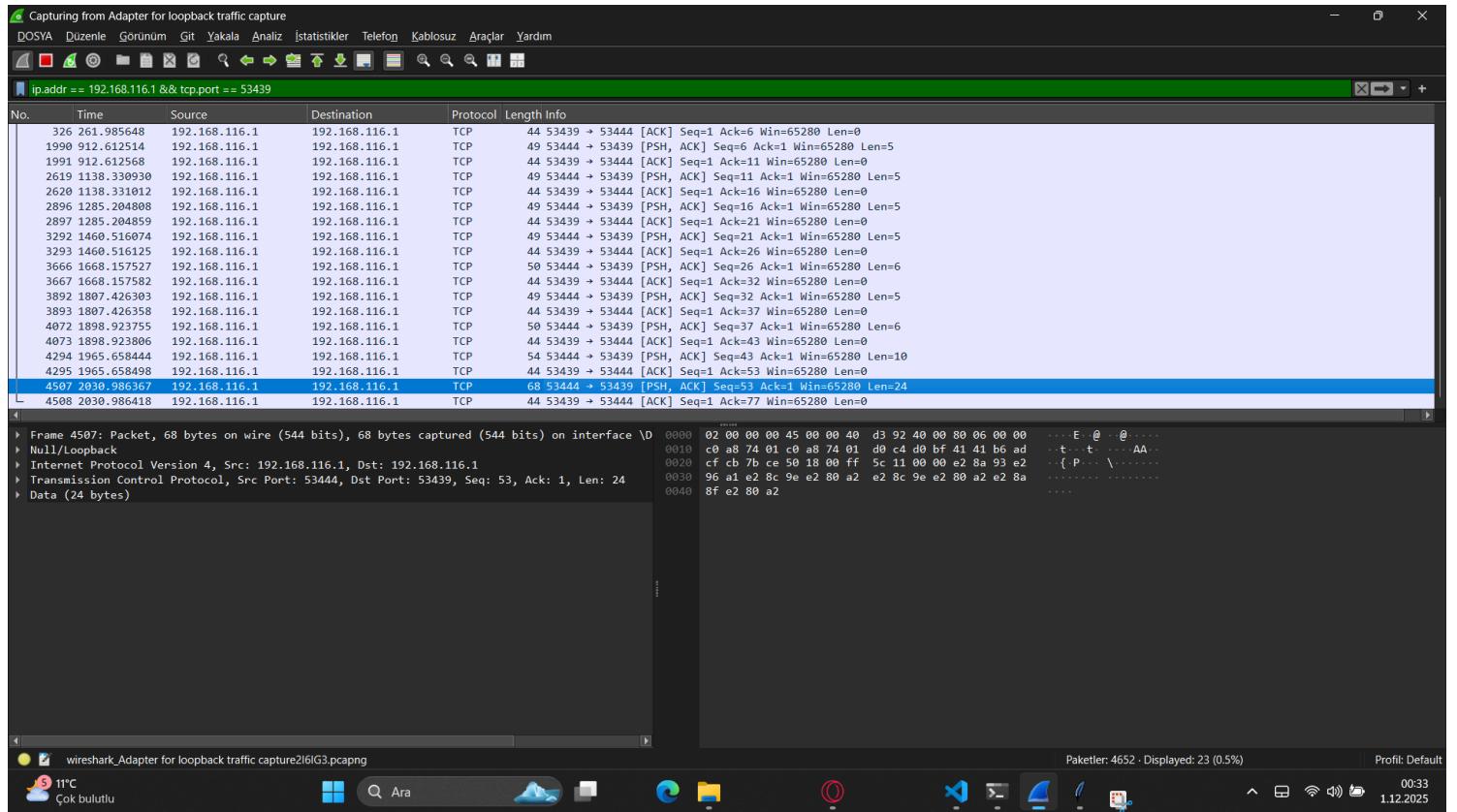
Algoritma Seç: Pigpen

Shift (Sezar): 3 Key / Parola: KEY

Affine A: 5 Affine B: 8

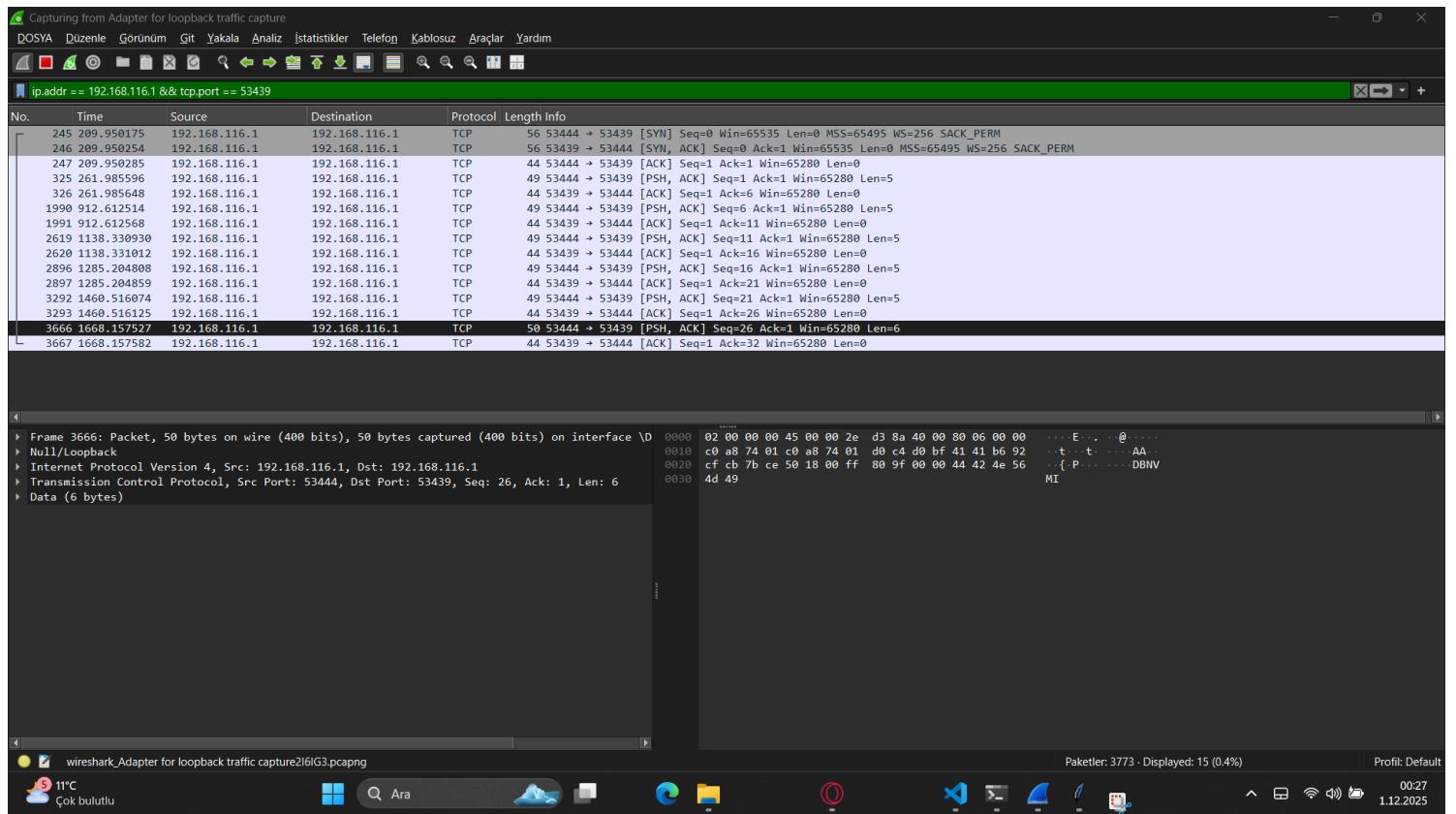
Rail / Sütun: 3

Şifrele ve Gönder



Pigpen sembollerle çalışır ama uygulamada genelde ASCII karşılığı kullanılır. HELLO mesajı Pigpen ile şifrelenince Wireshark'ta semboller veya sembollerin ASCII karşılıkları görünür. Mesaj hala okunabilir formdadır.

PLAYFAIR CIPHER



Playfair ile şifrelenen HELLO, Wireshark'ta harf çiftleri şeklinde şifreli metin olarak görünür. Wireshark içeriği plaintext gibi gösterir çünkü harflerden oluşur.

POLYBIUS CIPHER

Client - Güvenli Kripto Chat

- Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Columnar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Polybius): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç:	Polybius		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		

Server - Güvenli Dinième İstasyonu

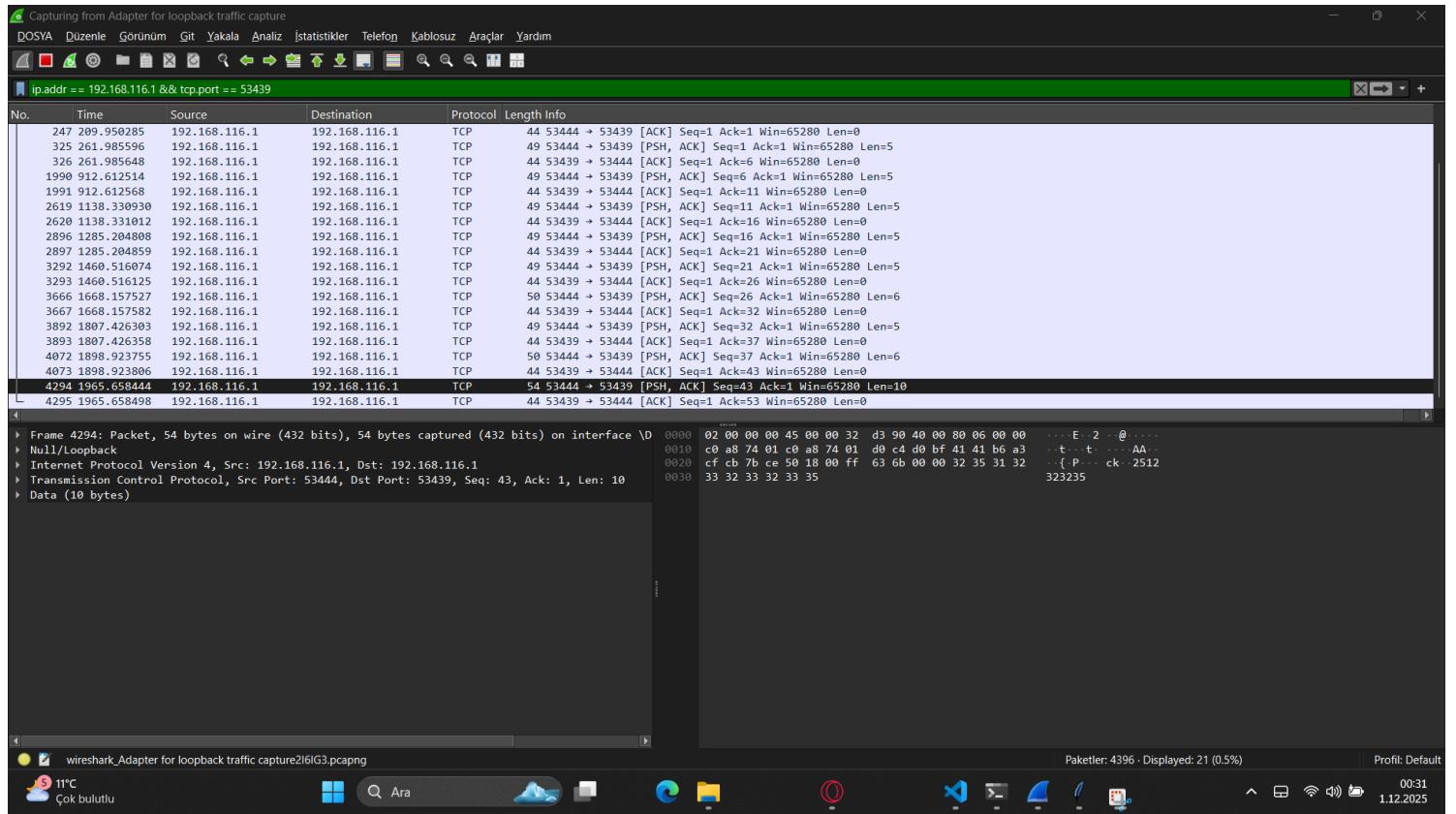
TÜM GEÇMİŞ ÇÖZÜLÜYOR

Mesaj #9 (2512323235) -> ⌂: HELLO

--- LİSTE SONU ---

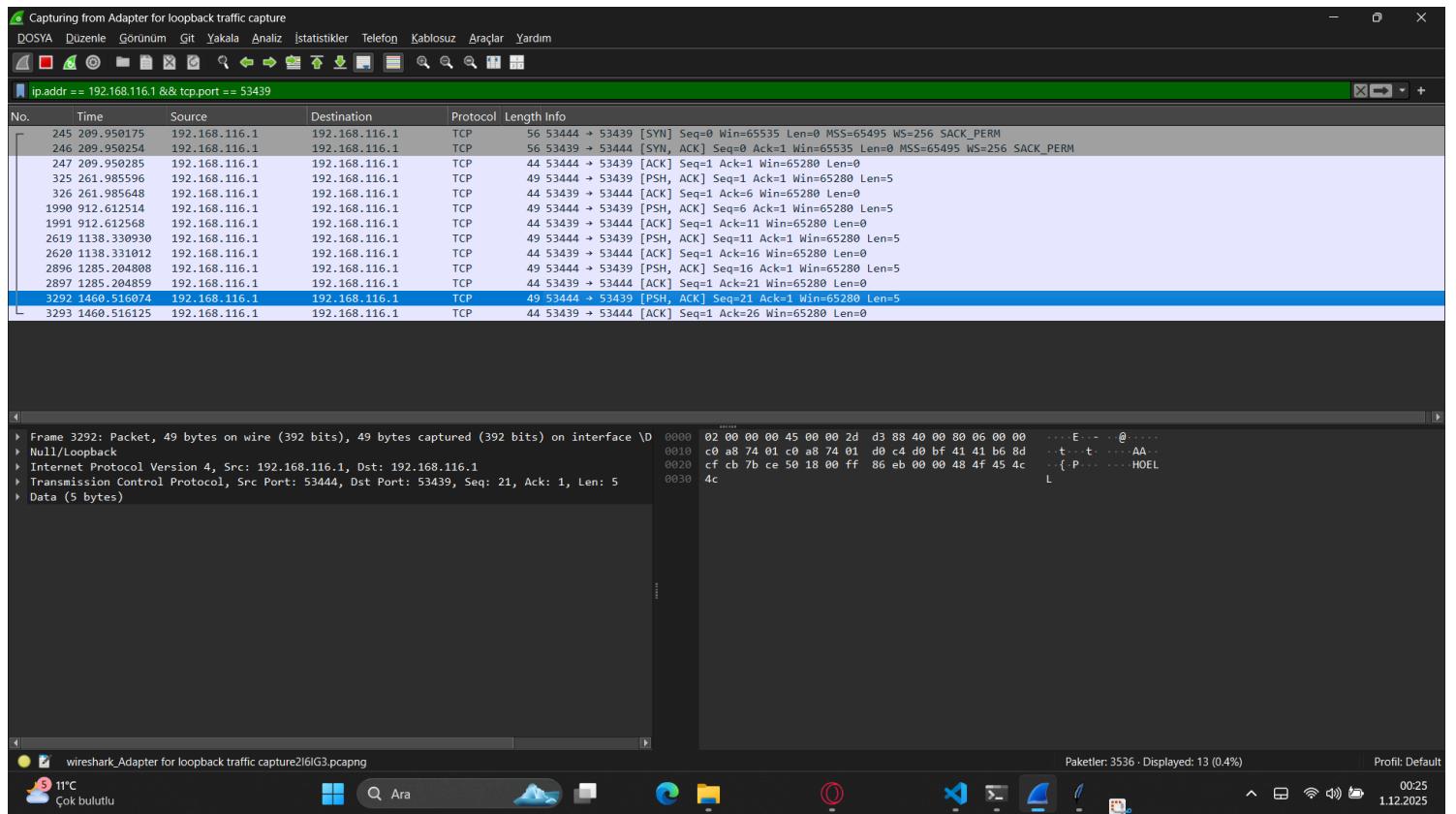
EKRANI TEMİZLE VE HEPİNİ ÇÖZ

Şifrele ve Gönder



Polybius kare ile şifrelenen HELLO mesajı Wireshark'ta 2 haneli sayılar dizisi (ör: 28 61 ...) olacak şekilde görünür. Wireshark bunu doğrudan okunabilir metin olarak gösterir.

RAIL FENCE CIPHER



HELLO Rail Fence ile şifrelenince Wireshark'ta harflerin yer değiştiirdiği ama hâlâ tamamen okunabilir bir çıktı görünür. Plaintext değil ama içeriği direkt okunabilir.

ROTATION CIPHER

Client - Güvenli Kripto Chat

- Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Server - Güvenli Dinleme İstasyonu

--- TÜM GEÇMİŞ ÇÖZÜLÜYOR ---

Mesaj #7 (URYYYB) -> : HELLO

--- LİSTE SONU ---

EKRANI TEMİZLE VE HEPŞİNİ ÇÖZ

Şifrele ve Gönder

Client - Güvenli Kripto Chat

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Şifrele ve Gönder

Server - Güvenli Dinleme İstasyonu

--- TÜM GEÇMİŞ ÇÖZÜLÜYOR ---

Mesaj #7 (URYYYB) -> : HELLO

--- LİSTE SONU ---

EKRANI TEMİZLE VE HEPŞİNİ ÇÖZ

Şifrele ve Gönder

Kriptografi Anahtarları

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Client - Güvenli Kripto Chat

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Şifrele ve Gönder

Server - Güvenli Dinleme İstasyonu

--- TÜM GEÇMİŞ ÇÖZÜLÜYOR ---

Mesaj #7 (URYYYB) -> : HELLO

--- LİSTE SONU ---

EKRANI TEMİZLE VE HEPŞİNİ ÇÖZ

Şifrele ve Gönder

Kriptografi Anahtarları

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Client - Güvenli Kripto Chat

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

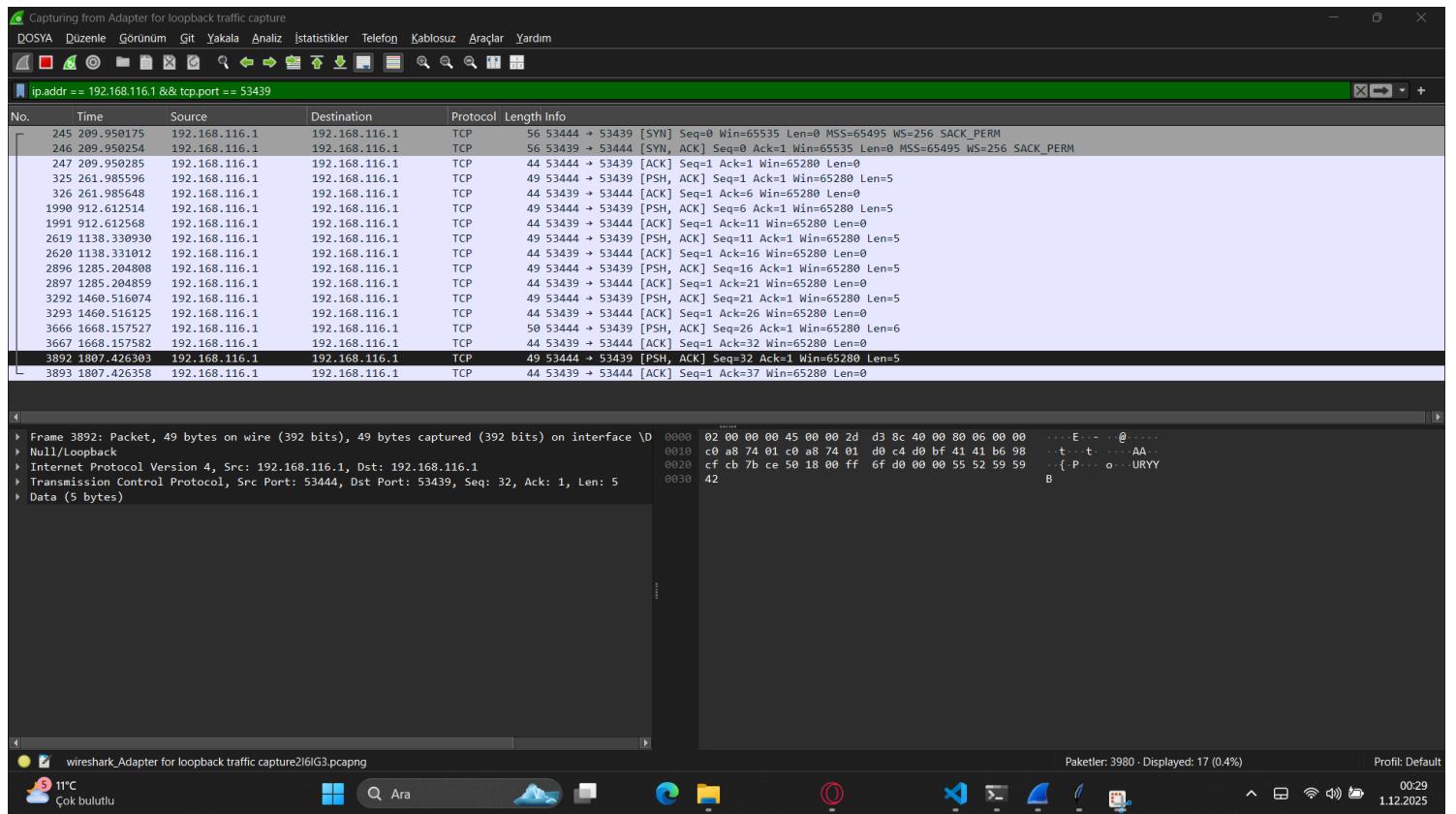
Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: **ROT13**

Shift (Sezar): **3** Key / Parola: **KEY**
 Affine A: **5** Affine B: **8**
 Rail / Sütun: **3**

Şifrele ve Gönder



HELLO Rail Fence ile şifrelenince Wireshark'ta harflerin yer değiştiirdiği ama hâlâ tamamen okunabilir bir çıktı görünür. Plaintext değil ama içeriği direkt okunabilir.

ROUTE CIPHER

Client - Güvenli Kripto Chat

- Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Affine): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (RailFence): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Playfair): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (ROT13): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Columnar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Polybius): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Fibonacci): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
- Ben (Route): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: **Route**

Shift (Sezar): 3	Key / Parola: KEY
Affine A: 5	Affine B: 8
Rail / Sütun: 3	

Server - Güvenli Dinleme İstasyonu

```

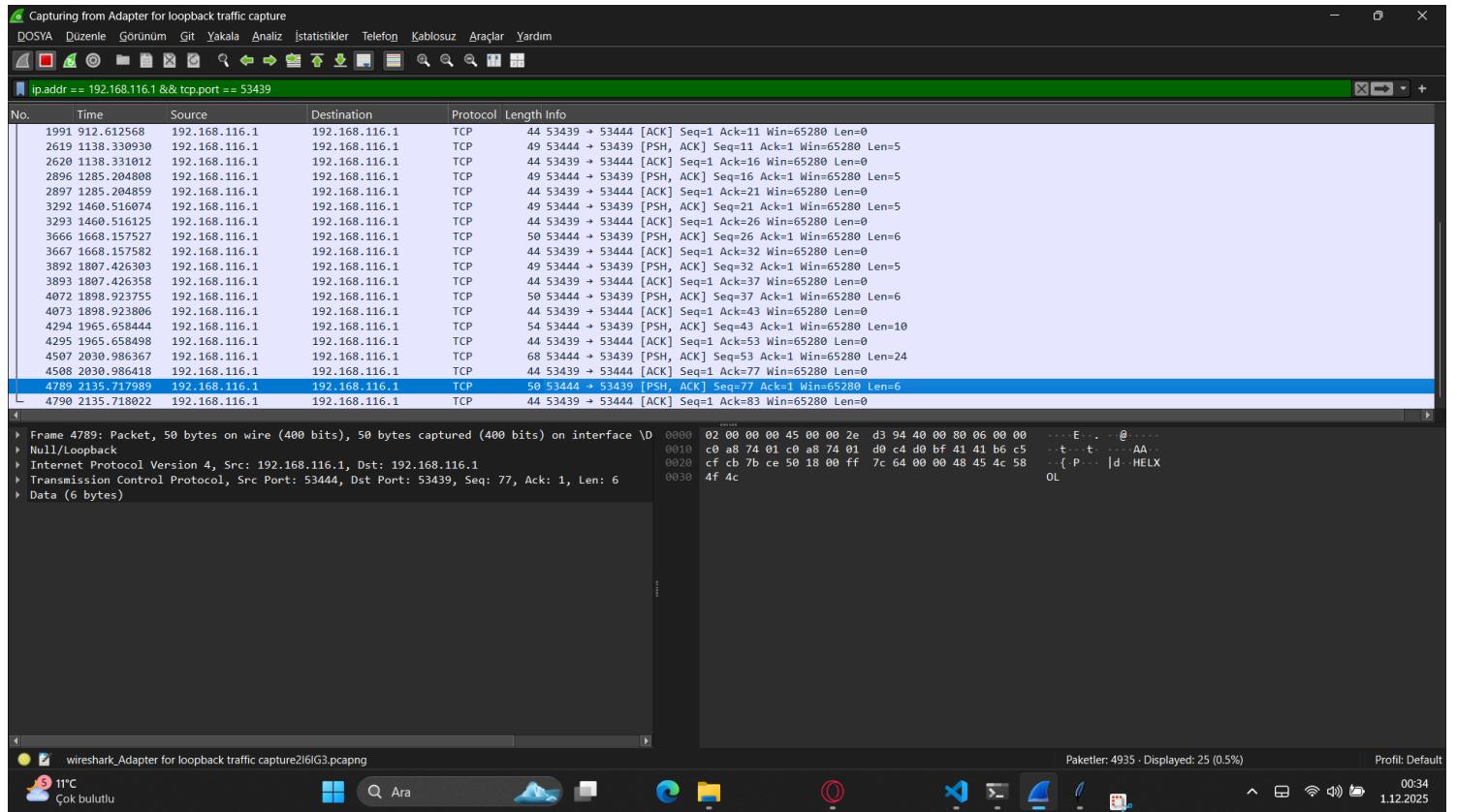
--- TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
Mesaj #11 (HEXLOL) -> : HELLO
--- LİSTE SONU ---

```

EKRANI TEMİZLE VE HEPİNİ ÇÖZ

Şifrele ve Gönder

11°C Çok bulutlu 00:29 11.12.2025



Route cipher ile şifrelenen HELLO mesajı Wireshark'ta harf sıralaması değişmiş şekilde plaintext olarak görünür. İçerik okunabilir ama şifreli.

RSA CIPHER

Server - Güvenli Dinleme İstasyonu

```
--- ⌂ TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
Mesaj #13 (3000,28,2726,2726,1307) -> ⌂: HELLO
--- LISTE SONU ---
```

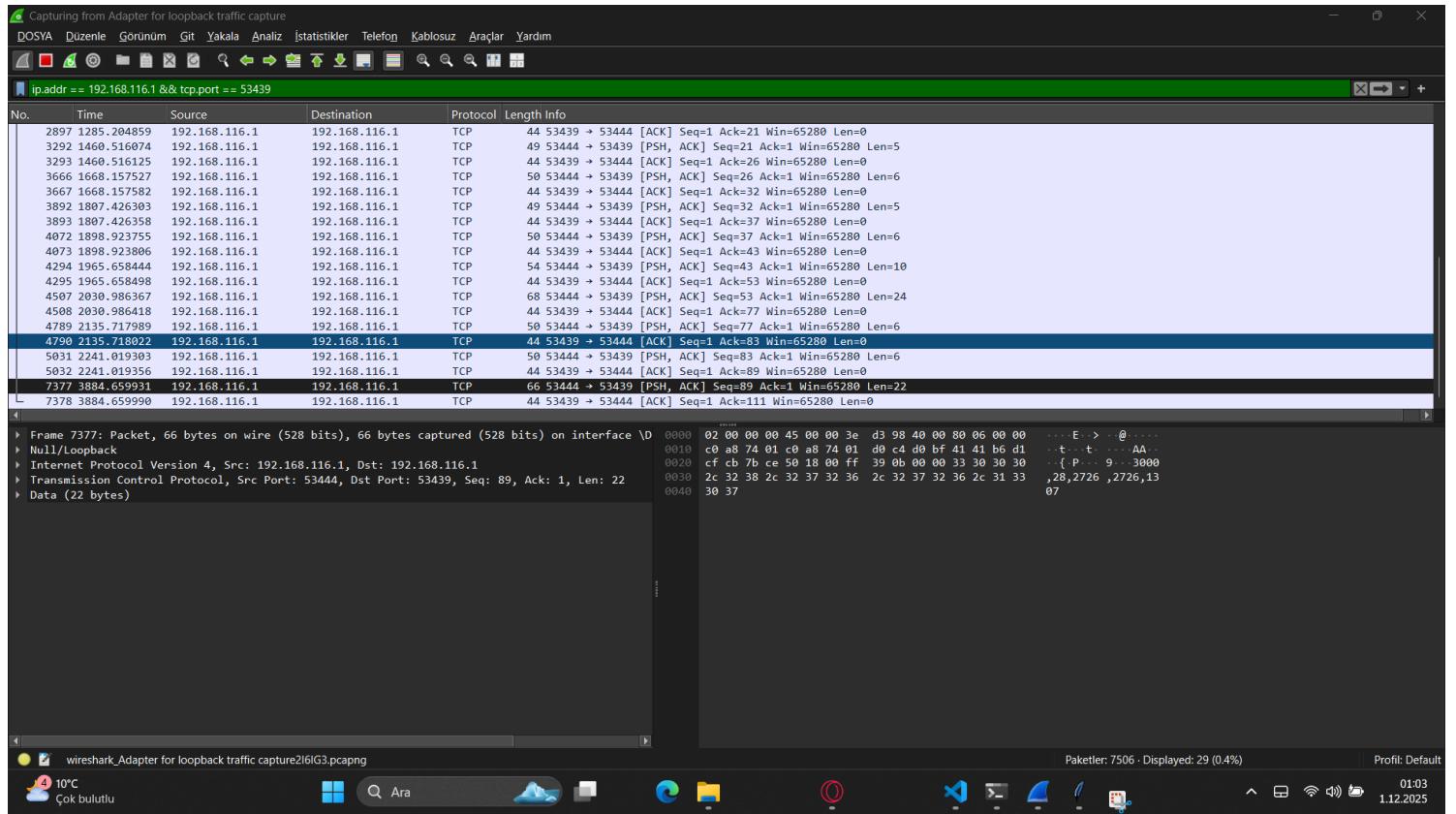
Client - Güvenli Kripto Chat

Kriptografi Laboratuvarı

Algoritma Seç:	RSA		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		

Kriptografi Anahtarları

Algoritma Seç:	RSA		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		



RSA ile şifrelenen HELLO mesajı Wireshark'ta büyük, rastgele görünen binary blok olarak görünür. Hiçbir ASCII okunamaz. Wireshark yalnızca ham cipher-text'i gösterir.

SEZAR CIPHER

--- @ TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
 Mesaj #1 (KHOOR) -> @: HELLO
 --- LISTE SONU ---

Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]

Kriptografi Laboratuvarı

Algoritma Seç: Sezar
 Shift (Sezar): 3 Key / Parola: KEY
 Affine A: 5 Affine B: 8
 Rail / Sütun: 3

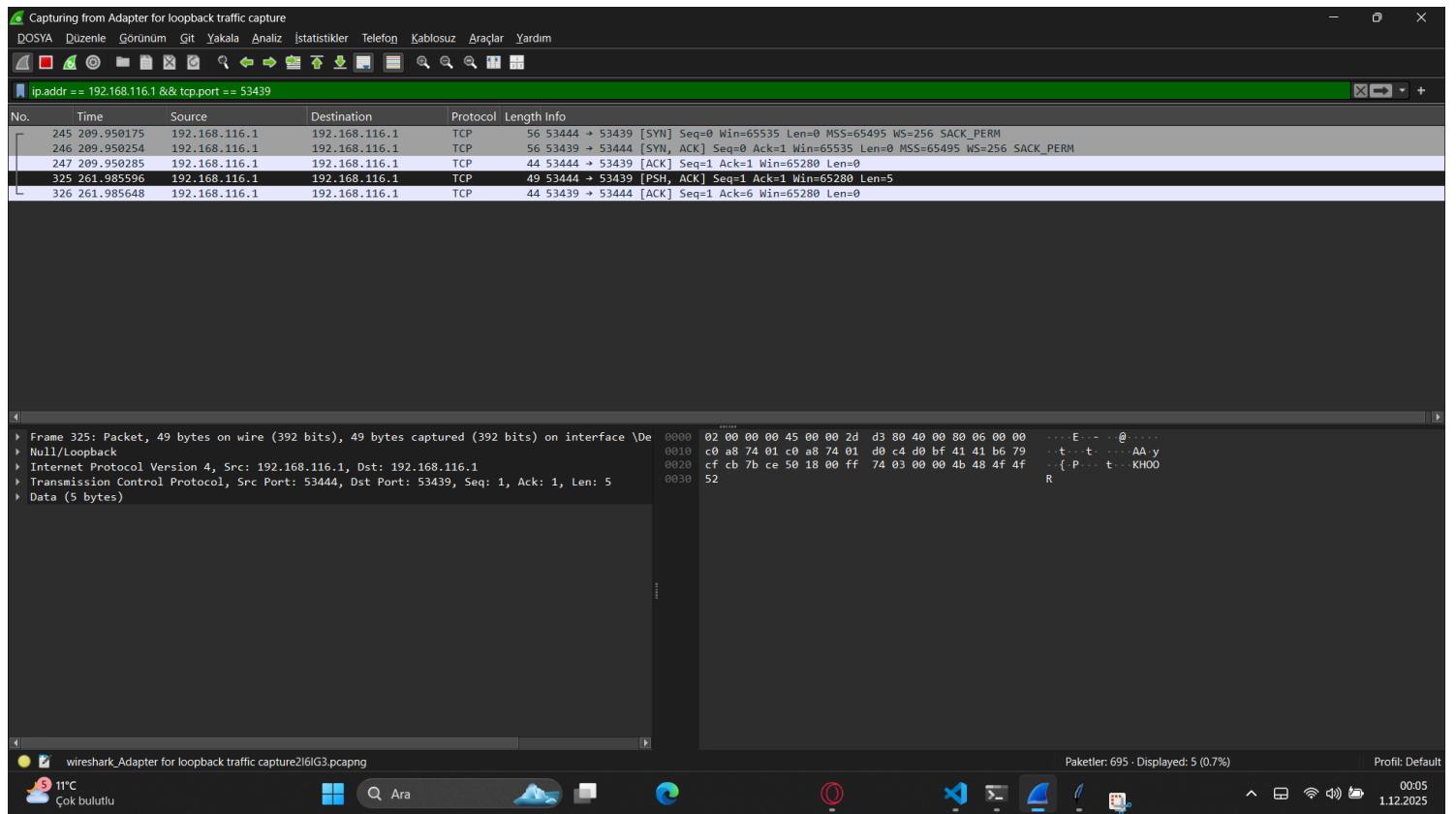
Şifrele ve Gönder

EKRANI TEMİZLE VE HEPİNİ ÇÖZ

Kriptografi Anahtarları

Algoritma Seç: Sezar
 Shift (Sezar): 3 Key / Parola: KEY
 Affine A: 5 Affine B: 8
 Rail / Sütun: 3

Şifrele ve Gönder



Sezar şifrelemesi HELLO'y'u Wireshark'ta kaydırılmış ama tamamen okunabilir bir metin olarak gösterir. Şifreli fakat plaintext formatında görünür.

SUBSTITUTION CIPHER

Server - Güvenli Dinième İstasyonu

```
--- ⌂ TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
Mesaj #3 (PQXXK) -> ⌂: HELLO
--- LISTE SONU ---
```

Client - Güvenli Kripto Chat

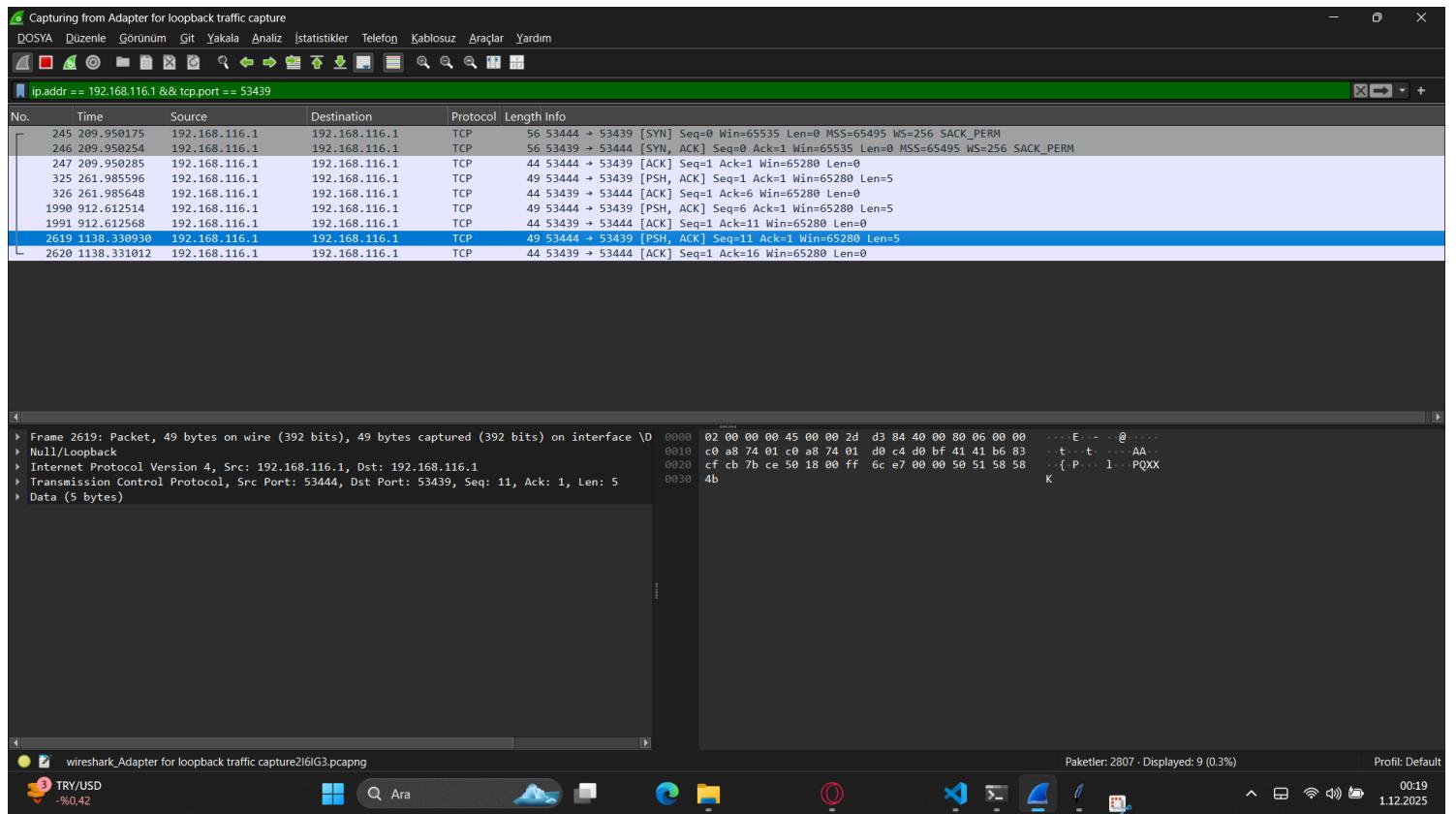
```
Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Substitution): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
```

Kriptografi Laboratuvarı

Algoritma Seç:	Substitution →		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		

Kriptografi Anahtarları

Algoritma Seç:	Substitution →		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		



Yerine koyma (Substitution) ile şifreli HELLO Wireshark'ta harflerin başkalarıyla değişmiş hâliyle görünür. Okunabilir, plaintext formundadır.

VIGENERE CIPHER

Server - Güvenli Dinleme İstasyonu

```
--- ⌂ TÜM GEÇMİŞ ÇÖZÜLÜYOR ---
Mesaj #2 (RIJVS) -> ⌂: HELLO
--- LİSTE SONU ---
```

Client - Güvenli Kripto Chat

```
Ben (Sezar): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
Ben (Vigenere): HELLO -> [ŞİFRELİ GÖNDERİLDİ]
```

Kriptografi Laboratuvarı

Algoritma Seç:	Vigenere		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		

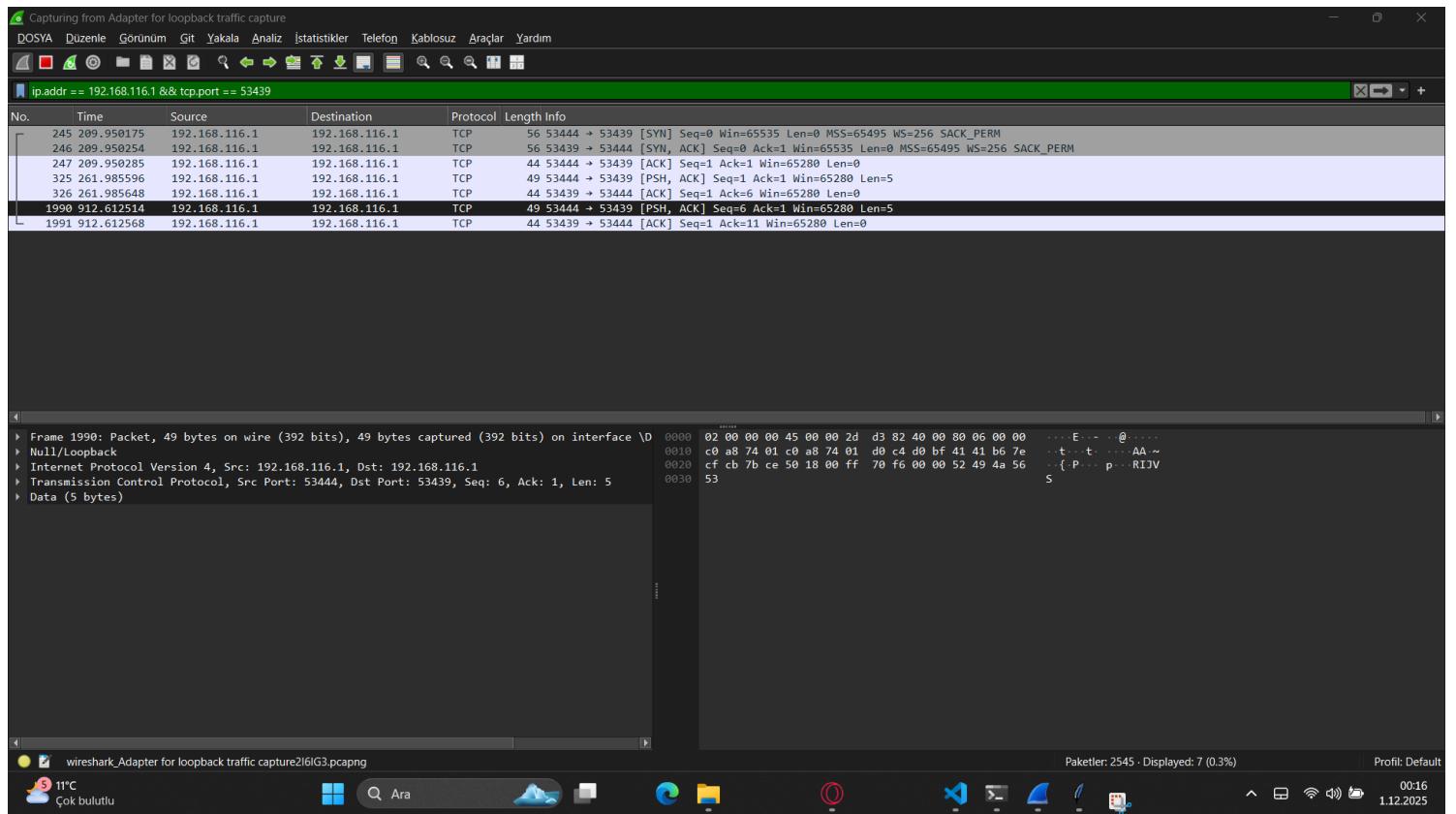
EKRANI TEMİZLE VE HEPİNİ ÇÖZ

Şifrele ve Gönder

Kriptografi Anahtarları

Algoritma Seç:	Vigenere		
Shift (Sezar):	3	Key / Parola:	KEY
Affine A:	5	Affine B:	8
Rail / Sütun:	3		

Şifrele ve Gönder



Vigenère ile şifrelenen HELLO Wireshark'ta karmaşık görünen ama yine alfabetik bir şifreli metin olarak görünür. Wireshark içeriği direkt plaintext gibi gösterir.

Bu çalışmada HELLO mesajı kullanılarak farklı şifreleme ve şifreleme benzeri algoritmalar test edilmiş ve her birinin ağ trafiği üzerindeki etkisi Wireshark ile analiz edilmiştir.