# DES ALGORİTMASI KULLANILAN AKILLI KART İLE GÜVENLİK SİSTEMİ TASARIMI ve UYGULAMASI

Oğuzhan URHAN Fevzi ZENGİN Musa ŞANLI

urhano@kou.edu.tr fevzizengin61@hotmail.com musanli@msn.com

Elektonik ve Haberleşme Mühendisliği Bölümü
Veziroluğu Yerleşkesi, Kocaeli Üniversitesi, 41040, KOCAELİ

## ÖZET

Bu çalışmada simetrik anahtarlı bir şifreleme sistemi olan DES (Data Encyription System) kullanılarak düşük maliyetli bir güvenlik sistemi geliştirilmiştir. Geliştirilen sistem bir terminal donanımı, bu donanım üzerinde çalışan yazılım, akıllı kart ve akıllı kartta çalışan yazılımdan oluşmaktadır. Akıllı kart içerisinde bir mikrodenetleyici ve EEPROM (Electrically Erasable Programmable Read-Only Memory) bulunmaktadır. Ayrıca kullanılan akıllı kartta bulunan mikrodenetleyicinin dahili EEPROM'u da mevcuttur. Dahili EEPROM'da DES şifreleme sistemine ait bilgiler ve kart sahibine ait özel bilgiler (tanıtım numarası-ID number) tutulmaktadır. Akıllı kartta ve terminalde bulunan mikrodenetleyicinin hem program belleği hem de dahili EEPROM veri belleği kod korumalı olduğundan üzerinde çalışan yazılım okunamamakta ve EEPROM'unda bulunan bilgilere erişlememektedir. Akıllı kartta bulunanan harici EEPROM'da ise genel erişime açık bilgiler tutulmaktadır. Akıllı kart ile terminal arasında yapılan haberleşme sırasında gönderilen bilgiler DES ile şifrelendiğinden haberleşme sırasında bu şifrelenmiş bilgiler 3. kişiler tarafından elde edilse bile bu bilgilerden gönderilen gerçek verinin elde edilmesi oldukça zordur. Akıllı kartın, terminalde her kullanılışında DES algoritmasında kullanılan anahtarın bazı bitleri değiştirilerek şifreli verinin kırılması daha da zorlaştırılmıştır.

## ŞİFRELİ HABERLEŞMEYE GENEL BİR BAKIŞ

İnsanoğlu eski çağlardan beri bilgiyi şifrelemeye uğraşmış ve birbirleri ile haberleşme için güvenli yollar aramıştır. Örneğin, antik mısırlılar bazı eserlerine şifreli hiyeroglif yazılar yazmıştır. 2000 yıl önce Julius Caesar ordusunun generalleri ile haberleşirken mesajlarında alfabedeki harflerin yerlerini değiştirmiştir. Caesar Cipher (Sezar şifresi) olarak bilinen bu yöntemde harflerin yer değiştirme sayısının K=3 olduğunu duruma alfabedeki harfler aşağıda verilen şekilde şifrelenecektir. Dikkat edilirse harfler 3 kez sola kaydırılmıştır.

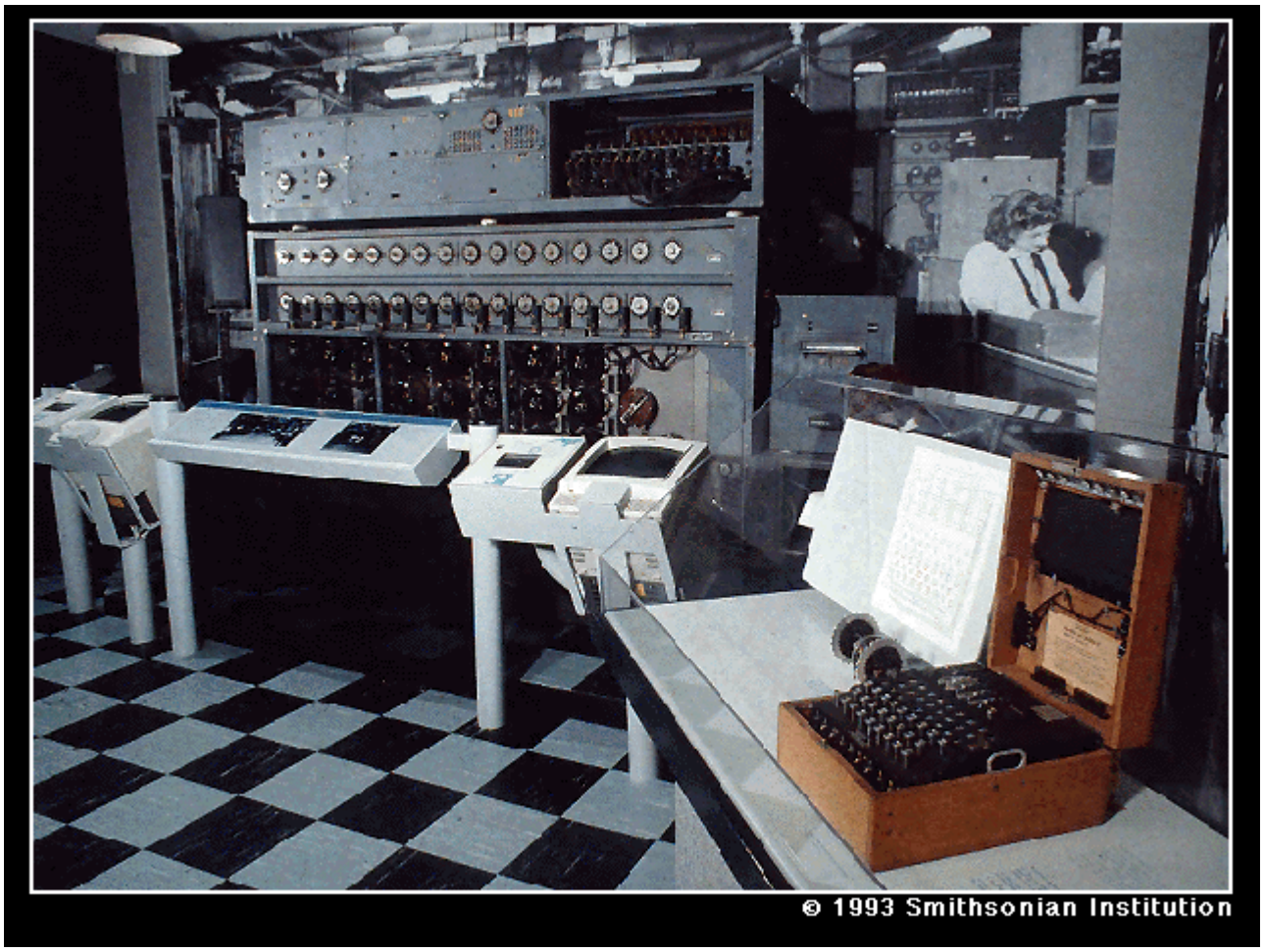
Şifrelenecek harf (Plaintext) : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Şifrelenmiş harf (Ciphertext) : DEFGHIJKLMNOPQRSTUVWXYZABC

Burada K şifrelemeyi sağlayan anahtardır. Şifreli haberleşecek her iki taraf da bu anahtarı bilmelidir. Örneğin şifreli bir mesaj göndermek isteyen kişi "KOCAELI UNIVERSITESI" sözcüğünü, K=3 kullanarak Sezar şifresi ile şifrelesin. Bu durumunda

Şifrelenecek metin : KOCAELI UNIVERSITESI
Şifrelenmiş metin : NRFDHOL XQLYHUVLWHVL

olarak elde edilmektedir. Şifrelenmiş metinden şifrelenmemiş metni elde etmek için mesajı alan taraf K=3 bilgisini sahip olduğundan şifrelenmiş metindeki harflerin yerlerini 3 kez sağa kaydırarak asıl metni elde eder. Ancak K=3 bilgisine sahip olmayan 3. bir kişi, şifrelenmiş metinden, 1 ile 25 arasında değişen olası bütün K değerlerini deneyerek asıl metni elde edebilir. Bu yöntem kaba kuvvet saldırısı (brute force attack) olarak bilinir. Ayrıca daha uzun metinlerde harflerin sıklık analizi yapılarak K anahtarı bulunabilir. Sezar şifresi en basit şifreleme yöntemlerinden biridir.

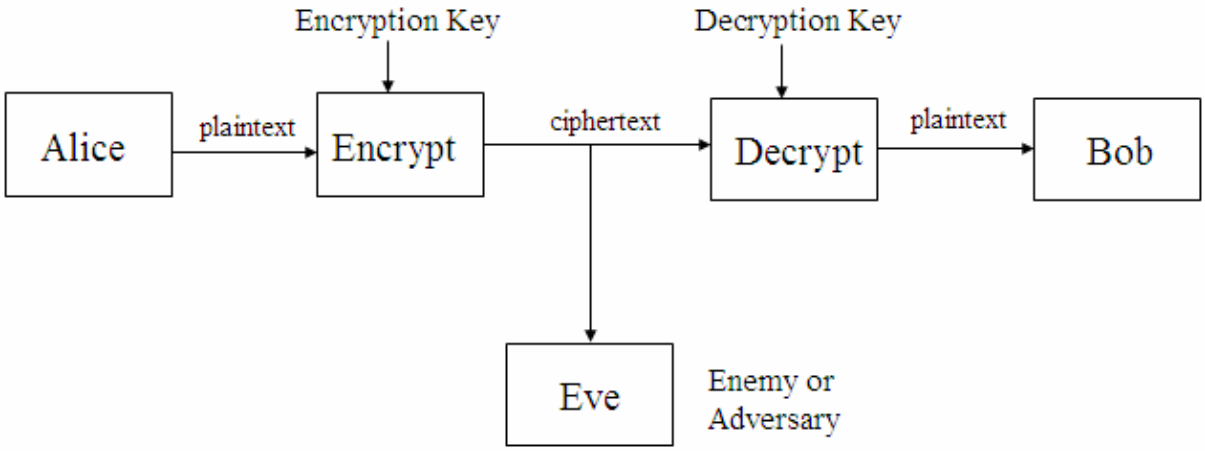
Güvensiz haberleşme kanalları üzerinden yapılmak istenen güvenli haberleşme önceleri askeri amaçla kullanılmaktaydı. Almanlar tarafından geliştirilen mekanik Enigma cihazı 2. Dünya Savaşı sırasında yoğun şekilde kullanıldı ve bu cihaz ile şifrelenen metinlerin ingilizler tafarından geliştirilen Bombe adlı cihazla çözülmesi ile savaşın kaderini etkiledi.




Şekil -1 Enigma ve Bombe cihazları (sağ taraftaki Enigma , arka plandaki Bombe)

Güvensiz kanallar üzerinden yapılmak istenen güvenli haberleşme senaryosu Şekil-2'de gösterilmektedir. Orjinal metni (plaintext) göndermek isteyen Alice şifreleme anahtarını (encryption key) kullanarak şifrelenmiş metni (ciphertext) elde eder ve bu metni Bob'a yollar. Şifreli metni alan Bob, şifre çözme anahtarını (decryption key) kullanarak orijinal metni (plaintext) elde eder. Haberleşme kanalını dinleyen Eve ise sadece şifrelenmiş metni elde edebilir.

Şifreleme sistemleri anahtar yapısına göre temel olarak ikiye ayrılır. Şifreleme ve şifre çözme anahtarının aynı olduğu şifreleme sistemleri simetrik veya gizli anahtarlı (private key cryptosystem) şifreleme sistemleri olarak adlandırılırken şifreleme ve şifre çözme anahtarının farklı olduğu sistemler asimetrik veya açık anahtarlı şifreleme (public key cryptosystem) sistemleri olarak adlandırılır.




Şekil-2 Temel haberleşme senaryosu

20. yüzyılın son çeyreğine kadar bilgiyi şifrelemek ve çözmek için tek anahtardan yararlanılan simetrik şifreleme sistemleri kullanıldı. Simetrik anahtarlı şifreleme sistemleri temel olarak çeşitli yer değiştirme ve permütasyon işlemlerine dayanmaktadır (Sezar şifresi gibi). Simetrik anahtarlı şifreleme sistemlerinin en bilineni ise IBM tarafından geliştirilen DES (Data Encryption Standart) yöntemidir.

Açık anahtarlı şifreleme sistemlerinin temelini Diffie ve Hellman atmıştır. Bu bilim adamları 1976 yılında yayınladıkları bir makale ile açık anahtarlı şifreleme sistemini önermiş ve araştırmacılara bu mantığı kullanan şifreleme sistemleri geliştirmeleri konusunda çağrıda bulunmuşlardır. Ron Rivest, Adi Shamir ve Len Adleman 1977 yılında bu mantığı kullanan bir şifreleme tekniği geliştirdiler ve bunu 1978 yılında bir yayına dönüştürdüler [1]. Bu yöntem geliştiricilerinin soyadlarının baş harfleri olan RSA olarak bilinmektedir.

Simetrik anahtarlı şifreleme sistemleri asimetrik şifreleme sistemlerine göre oldukça hızlı çalışmaktadırlar. Ancak veriyi şifrelemek ve çözmek için aynı anahtarın kullanılması sorun yaratmaktadır. Asimetrik anahtarlı şifreleme sistemlerinin işlem yükü ise oldukça fazladır. Bu nedenle uzun metinleri şifrelemek için genellikle simetrik şifreleme yöntemleri kullanılmakla birlikte kısa metinler için asimetrik şifreleme yöntemleri kullanılmaktadır. Her iki yöntemin birlikte kullanıldığı PGP (Pretty Good Privacy - Tatlı Mahremiyet) gibi melez (hibrit -hybrid) yöntemler de mevcuttur.

Bu çalışmada gömülü bir sistem (embedded system) kullanılarak şifreli haberleşme düşünüldüğünden kullanılacak algotirtmanın oldukça hızlı olması gerekmektedir. Bu amaçla simetrik şifreleme algoritmalarının en bilineni ve üzerinde en çalışılanı olan DES yönteminin kullanılması tercih edilmiştir. Bu yöntemin geliştirilmiş biçimleri hali hazırda birçok sistemde kullanılmaktadır.

## DES ALGORİTMASI

DES algoritması temel olarak basit mantıksal (lojik) işlemler kullanmaktadır. Yöntem, 64-bitlik veri bloklarını, 64-bitlik bir anahtarın 8. bitlerinin kullanmadan 56-bitlik anahtar kullanılarak şifreler. Yani kullanılabilecek anahtar sayısı $2^{56}$ = 72.057.594.037.927.936'dır (yaklaşık 72 katrilyon). Bu anahtarlardan çok az bir kısmı kullanılarak şifrelenen metinler kolayca çözülebilir. Bu anahtarlar zayıf anahtar (weak key) olarak adlandırılır. DES algoritmasının detayları [2] ve [3] kaynaklarından edinilebilir.

1998 yılında EFF (Electronic Frontier Foundation) DES algoritmasını olası bütün anahtarları deneyerek (kaba kuvvet saldırısı-brute force attack) ortalama 4.5 günde kırabilecek bir donanım geliştirdiğini açıkladı. Jhon Gilmore liderliğindeki ekibin 220.000$ harcanarak geliştirdiği bu donanım saniyede 90 milyar civarıda şifreyi deneyebilmektedir. Şekil-3'de makinenin prensip tasarımcısı Paul Kocher üzerinde 64 yonga (microchip) bulunan 29 karttan biri ile görülmektedir. Bu sistemde 1800'den fazla yonga kullanılmıştır. Paul Kocher'in arkasında 6 kabinetten oluşan ve bir PC tarafından koordine edilen DES algoritmasını kıran sistemin tamamı görülmektedir.

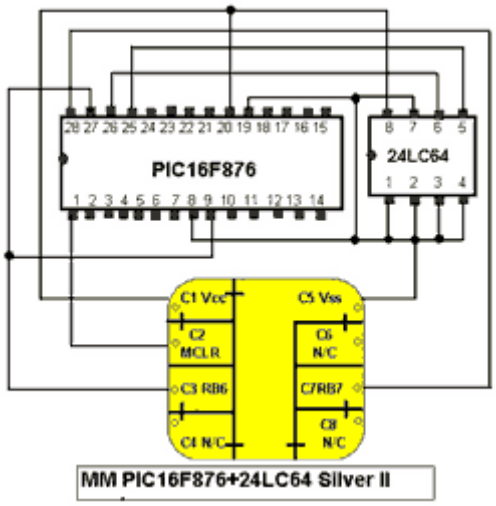
Şekil-3 DES algoritmasını kıran donanım

DES algoritmasının güvenli olmadığı ve anahtar boyutunun artırılması gerektiği Bruce Schneier tarafından daha önce dile getirilmişti [4]. DES ile şifrelenmiş verinin ikinci bir anahtarla şifre çözme işlemine tabii tutulması ve elde edilen bu verinin tekrar farklı bir anahtarla tekrar şifrelenmesi ile oluşan 3-DES (triple-DES,üçlü-DES) algoritması, DES algoritmasından $2^{56}$ kat daha güçlüdür. Başka bir değişle kaba kuvvet atağı ile DES algoritmasını 1 saniyede kırılabilen bir sistemin 3-DES algoritmasını kırması 2 milyar yıldan fazla sürer. Bruce Schneier bu durumu "Bu galakside 3-DES'i kaba kuvvet atağı ile

kırabilecek kadar silikon veya güneş yok olmadan önce kırabilecek kadar zaman yok" sözü vurgulamıştır.

## GÜVENLİ ANAHTAR GÜNCELLEMELİ DES ALGORİTMASININ UYGULANMASI

DES şifreleme sistemi kullanılarak tasarımlanan güvenlik sistemi, güvenlik (geçiş) noktalarında bulunan bir akıllı kart terminal donanımı ve kullanıcılarda bulunan akıllı kartlardan oluşmaktadır. Terminalde Microchip firması tarafından geliştirilen PIC16F877 adlı mikrodenetleyici kullanılmaktadır. Akıllı kartın içinde ise PIC16F877 mikrodenetleyicisi ve 24LC64 EEPROM'u bulunmaktadır. Şekil-4'de akıllı kartın PIC16F876 ve 24LC64 içeren şeması verilmiştir. Bu uygulamada PIC16F877 mikrodenetleyicisini içeren akıllı kartlar kullanılmıştır.




Şekil-4 PIC16F876 ve 24LC64 içeren bir akıllı kartın iç yapısı

Akıllı kartın dış görünüşü Şekil-5'de verilmiştir. Bir kredi kartı büyüklüğündeki kartın dış dünya ile haberleşmek için sadece bir giriş/çıkış ucu bulunmaktadır. Bu nedenle terminalle haberleşmek için tek hattan çift yönlü haberleşilebilinen bir protokol geliştirilmiştir. Bu giriş/çıkış ucu dışında kartın temas noktalarında mikrodenetleycinin ve harici EEPROM'un besleme uçları, mikrodenetleyicinin programlama ve saat işareti girişi bulunmaktadır.


Şekil-5 Kullanılan akıllı kartın dış görünüşü

DES algoritmasının yukarıda anlatıldığı gibi kırılması mümkün olduğundan şifreleme ve şifre çözme için kullanılan anahtarın belirli bitleri her oturumda güncellenmektedir. Yani DES için

kullanılan şifrenin belirli bir kısmı (belirli 48-biti) sabit seçilmiştir. Anahtarın sabit kısmı hem terminalde hem de akıllı karttaki PIC16F877'nin dahili EEPROM'una yazılmıştır. Bu bellek bölgesi kod korumalı olduğundan okunmaz. Dolayısıyla DES anahtarının sabit kısmı güvencededir.

Şifrenin değişen kısmı, akıllı kart terminale her sokulduğunda terminalden akıllı karta gönderilen 64-bitlik rasgele sayının belirli 16-biti kullanılarak oluşturulmaktadır. Bu 16-bitlik şifre bilgisinin rasgele sayı içerisindeki yeri ve bu şifre bilgisinin oturum şifresini oluşturma şekli hem terminal hem kart tarafından bilindiğinden 64-bitlik rasgele veri akıllı karta ulaştığı anda her iki tarafta yeni oluşturulan oturum şifresi ile güvenli bir şekilde haberleşmeye hazırdır.

Geliştirilen sistemde herbir kullanıcı grubu için 64-bitlik tanıtım numası (ID number) tanımlanmıştır. Akıllı kart ile terminal oturum şifresi üzerinde anlaştıktan sonra akıllı kartta bulunan PIC16F877, dahili belleğinde tuttuğu 64-bitlik tanıtım numarası bilgisini oturum anahtarı ile şifreleyip terminale yollar. Terminal şifrelenmiş tanıtım numarası bilgisinden orijinal tanıtım numarasını elde ederek o akıllı kartın sisteme dahil olup olmadığını ve güvenlik noktasından geçiş hakkına sahip olup olmadığını belirler. Bu işlem 1sn'den kısa sürede yapılmaktadır.

Terminal ile akıllı kartın haberleşmesi durumunda hattı dinleyen kötü niyetli 3. kişi (Şekil-2'deki Eve) hem DES ile şifrelenerek gönderilen tanıtım numaralarını hem de şifreleme için kullanılan anahtarı bilmediğinden orijinal bilgiyi elde edemez. Ayrıca veriyi şifreleme için kullanılacak oturum anahtarının 16 biti her oturumda değiştiğinden şifreli verinin elde edilmesi daha da zorlaştırılmıştır.


Şekil-6 Tasarımlanan akıllı kart terminali

Tasarımlanan akıllı kart terminali Şekil-6'da görülmektedir. Akıllı kartlarda ve terminallerde bulunan mikrodenetleyicilerin program ve dahili EEPROM bellekleri kod korumalı olduğundan sistemin kopyalanması da mümkün değildir. Ayrıca güvenlik noktasından yapılan geçişlere ait bilgilerin RS-232 protokolü ile bir bilgisayara da aktarılabilmesine olanak sağlayan arabirim terminal donanımı üzerinde mevcuttur. Böylece hangi güvenlik noktasından kimlerin hangi tarih ve saatte geçtiği belirlenebilir. Bu sistem, yazılımda yapılacak değişiklikler ile kontör ve para gibi diğer özel bilgiler de saklayabilir. Tasarımlanan sistemin terminal donanımsal maliyeti 25$'ın altındadır. Bir akıllı kartın maliyeti ise birkaç dolar civarındadır. Terminal ve akıllı kartlar için geliştirilen yazılım CC5X C derleyicisi kullanılarak yazılmıştır.

## KAYNAKLAR


[1] R.L. Rivest, A. Shamir, L.M. Adleman , "A method for obtaining digital signatures and public-key cryptosystem", Communications of the ACM, 21(2) , 120-126, February 1978.
[2] A. Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/about/chap7.pdf
[3] http://mf.kou.edu.tr/elohab/oguzhan/kripto. Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Ağ ve Veri Güvenliği Ders Notları, 2004. (06.08.2004)
[4] B. Schneier , "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons Inc., 1994.
[5] http://public.planetmirror.com/pub/descrack/faq.html. (06.08.2004)
[6] B. Schneier, "A Hardware DES Cracker", Crypto-Gram Newsletter, 15 August 1998. http://www.schneier.com/crypto-gram-9808.html (06.08.2004)
[7] O. Urhan ve M.K. Güllü, "Her Yönüyle PIC16F628", Birsen Yayınevi, İstanbul, ISBN 975-511-371-1, 2004.
[8] CC5X User Manual v3.0 and v3.1 http://www.bknd.com (06.08.2004)
[9] PIC16F87X Datasheet, http://www.microchip.com (06.08.2004)
[10] M. Toptaş , "Akıllı Kartlar ve Güvenliği", Bitirme Tezi, Kocaeli Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümü, 2004.

Jhon Gilmore – DES algoritmasını kıran donanımı geliştiren ekibin lideri


Bruce Schneier – Şifreleme konusunda yaptığı çalışmalar ve yazdığı kitaplarla tanınan Bruce Schneier, Economist dergisi tarafından bir güvenlik gurusu (security guru) olarak tanıtılmaktadır.