Özgün Bir Şifreleme Algoritması Kullanan Güvenli E-Posta Uygulaması

Muhammet Serkan Çinar, Işıl Çinar, Hasan Şakir Bilge

***Özet*—Bu çalışma ile her geçen gün yaygınlaşmakta olan yüksek kapasiteli ve ücretsiz olarak dağıtılan e-posta hizmetlerinin daha güvenilir kılınması amaçlanmıştır. E-posta işlemleri için bilinen ve yaygın kullanılan şifreleme algoritmalarının dışında yeni bir şifreleme algoritması tasarlanmıştır. Tasarlanan şifreleme algoritmasıyla geliştirilen e-posta uygulaması, güvenlik konusunda getireceği avantajların yanında, ücretsiz e-posta servis sağlayıcılarının izin verdiği ölçüde sunuculara erişmekte ve yapılan konfigürasyonlara göre istenilen hesabın tüm e-posta verilerini kendi veritabanına yükleyebilmektedir. Ayrıca şifreleme algoritması MS Outlook programına eklenti olarak geliştirilen başka bir uygulamaya da entegre edilerek kurumsal e-posta iletiminde de güvenli e-posta gönderilmesi sağlanmıştır. Her iki uygulamada da şifreleme algoritması başarılı bir şekilde gerçekleştirilmiştir.**

***Anahtar Kelimeler*— E-posta Güvenliği, POP3 ve SMTP Protokolleri, Simetrik Şifreleme.**

Secure Email Application Using an Original Encryption Algorithm

***Abstract*—In this study, email services which are distributed free with high storage capacity and which become widespread every day is intended to made more reliable. A new encryption algorithm is designed for email operations which is out of the known and widely used email encryption algorithms. Besides the advantages of security issues of the email application that is developed with proposed encryption algorithm, mail application can access to the email servers to the extent permitted by free email service providers and all of the data in desired email account can be downloaded into application database according to configurations. Furthermore, the encryption algorithm has been integrated into the add-in application developed for MS Outlook program and by this way the secure message sending is provided for organizational email transmissions. The encryption algorithm was implemented successfully for both applications.**

***Keywords*— Email Security, POP3 and SMTP Protocols, Symmetric Encryption.**

I. GİRİŞ

Sürekli artmaya devam eden bilgi ve beraberinde getirdiği bilgi değişimi iş sürekliliğinde ve kurumların gelişmesinde büyük rol oynamaktadır. Bilgi değişiminde birçok metot bulunmasına rağmen; e-posta tüm kurumlar için iletişim araçları arasında ilk sırada gelmektedir [1].

Günümüzde e-postalar kurumsal iletişimin yanında bireysel iletişim için de vazgeçilemeyecek derecede önemli bir haberleşme aracıdır. İletişimin yüksek oranlarda e-postalar aracılığıyla yapılması, bu iletişim üzerinden yapılan saldırıların da artmasına sebep olmuştur. Kurumların, şirketlerin, bireysel kullanıcıların e-posta güvenliği konusunda önlem almaları ihtiyaç haline gelmiştir [2].

İncelenen çalışmalarda e-posta sistemleri güvenliği konusu genel olarak işletim sistemi seviyesinde, e-posta uygulaması seviyesinde ve ağ altyapısı seviyesinde ele alınmakla birlikte; e-posta sunucusu ve istemci arasındaki iletişimin güvenliği, güvenli oturum yönetimi, basit ve kriptografik anahtarlar, onay mesajları ile e-posta takibi, spam mesajların elenmesi, zararlı e-posta takibi gibi güvenlikle ilgili çok farklı konularda çalışmalar yapıldığı görülmüştür [3,4,5,6].

Yapılan bu çalışmada, e-posta sistemlerinin uygulama seviyesindeki güvenliği dikkate alınarak özgün bir algoritma ile şifreleme işlemi gerçekleştirilmektedir.

Bu çalışmada özellikle literatürde karşılaşılan [7, 8] saldırganın gönderici ile alıcı arasında mesaj trafiğini dinleyebiliyor olması ve mesajı değiştirebilmesi, e-postaların şifresiz olarak sunucu ve bilgisayarlarda tutuluyor olması ve genel olarak kullanıcı hataları ile donanım/yazılım açıklıkları gibi tehditlerin engellenmesi hedeflenmiştir.

Bulut bilişim ile kullanıcı verilerinin büyük bir kısmının bulut üzerinde olacağı öngörülmekle birlikte, yüksek kapasiteli ücretsiz e-posta sağlayıcılar da kullanıcıları için bir bulut ortamı sağlamaktadırlar. Bulut bilişim servis modellerinden servis olarak sunulan yazılım (Software as a Service) yaklaşımında kullanıcıların servis sağlayıcıların bulut altyapısını kullanarak web tabanlı e-posta uygulamalarına farklı cihazlardan, farklı arayüzlerle erişebilmeleri mümkün kılınmaktadır. Bu yaklaşımda, kullanıcıya özgü sınırlı konfigürasyon ayarlamaları yapılabilmekte olup kullanıcının depolama ortamını, işletim sistemlerini ve ağ altyapısını kontrol etmesi veya yönetmesi mümkün olmamaktadır [9].

Kullanıcılar tüm e-posta verilerini bulut üzerine taşıdıklarında bazı özel gizlilik dereceli verilerinin şifreli olarak bu e-posta servis sağlayıcılarında tutulmasını isteyebileceklerdir. Ücretsiz olarak sağlanan bu yüksek kapasiteli ve hizmet devamlılığı olan e-posta hizmet sağlayıcıları bu bilgileri bağlı bulundukları devletin güvenlik birimleri veya üçüncü şahıslar ile paylaşabileceklerini belirtmekle beraber istedikleri zaman kullanıcılarının hesaplarını kapatabileceklerini kullanıcı sözleşmelerinde ifade etmektedirler. Bu açılardan bakıldığında son kullanıcılar için bu ücretsiz e-posta servis sağlayıcılarının sunucularında e-posta verilerinin şifreli tutulması ve yalnızca anahtarlarını paylaştıkları kişilerle şifreli e-posta iletimlerini gerçekleştirmeleri, kişisel bilgilerinin

M.S.Çinar,Hacettepe Üniv.Bilg.Müh., e-posta:(mscinar@hacettepe.edu.tr).
I.Çinar Gazi Üniv.Bilg.Müh., e-posta: (isil.cinar@gazi.edu.tr).
H.Ş.Bilge,Doç.Dr.,Gazi Üniv.Bilg.Müh.,e-posta:(bilge@gazi.edu.tr).

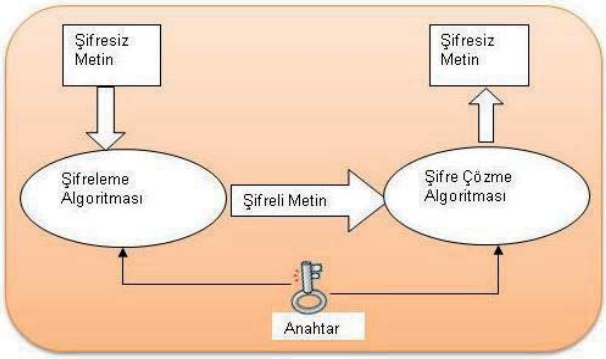
mahremiyetinin korunması hususunda önemli bir güvenlik mekanizması sağlayacaktır.

Çalışmada önerilen yaklaşım uçtan uca her seviyede güvenliği sağlamaya yönelik olarak önerilmiş bir çözüm olmamakla beraber, e-posta mesajları şifrelemesinin yaygın olarak kullanılan şifreleme algoritmaları dışında farklı bir algoritma ile sağlanmasını hedeflemiştir. Literatürde yapılan araştırmalarda simetrik şifrelemede DES, 3DES, AES ve Blowfish [10,11,12] algoritmalarının yaygın olarak kullanıldığı görülmüştür. E-posta güvenliğine yönelik simetrik şifreleme algoritmaları kullanarak yapılan çalışmalarda ise genellikle bahsedilen simetrik şifreleme algoritmaları kullanıldığı gözlemlenmiştir. Bu çalışmada ise farklı şifreleme teknikleri algoritmanın farklı adımlarında uygulanarak özgün bir simetrik şifreleme algoritması geliştirilmiştir.

Çalışmanın ikinci bölümünde geliştirilen simetrik şifreleme algoritmasından bahsedilmekte, üçüncü bölümde e-posta gönderme ve alma için gerekli protokollerin açıklaması yapılmakta ve bir sonraki bölümde de geliştirilen e-posta uygulamaları anlatılmaktadır. Beşinci bölümde gelecekte yapılması planlanan çalışmalar özetlenmektedir. Son olarak çalışmadan elde edilen kazanımlar ve sonuçlar sunulmuştur.

II. E-Posta İçerik Şifreleme Algoritması

Şifreleme algoritmasında gizli anahtarlı şifreleme yöntemi kullanılmıştır. Gizli anahtarlı şifreleme yönteminde, hem şifreleme hem de şifre çözme işlemi için aynı anahtar kullanılmaktadır. Bu yöntem simetrik şifreleme olarak da adlandırılmaktadır. Simetrik şifrelemede anahtarın alıcı tarafına güvenli bir şekilde iletilmesi önemlidir. Anahtar olmadığı sürece şifrelenmiş metin ele geçirilse de asıl metnin elde edilmesi mümkün değildir [13]. Şekil 1'de simetrik şifreleme algoritmalarının çalışma yapısı ana hatlarıyla gösterilmektedir.

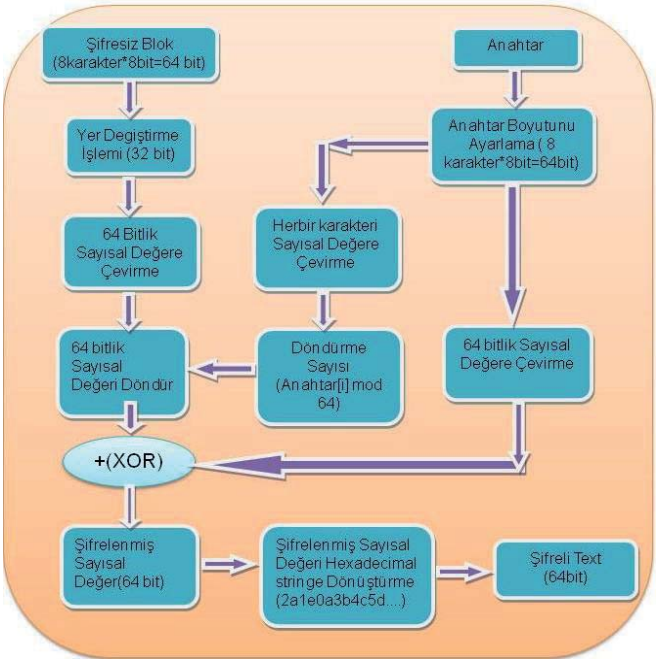


Şekil 1. Simetrik şifreleme algoritması çalışma yapısı

A. *Şifreleme Algoritması*

Çalışmanın bu bölümünde geliştirilen algoritmada uygulanan şifreleme adımları ele alınmış olup şifreleme algoritması Şekil 2'de akış diyagramı olarak sunulmuştur.

1) Şifreleme algoritması her bir 8 karakterin blok olarak alınıp, 8 karakterlik dizinin 64 bitlik sayısal değere dönüştürülmesi ve bu değerin bit seviyesinde çeşitli fonksiyonlardan geçirilmesini kapsamaktadır.
2) Şifreleme işlemine gelen 8 karakterlik dizi ilk olarak yer değiştirme işlemine tabi tutulur. İlk 4 karakter ve son 4 karakter yer değiştirir.
3) Yer değiştirme işleminden sonra 8 karakterlik blok 64 bitlik sayısal bir değişkene aktarılır. İlk karakter 64 bitin ilk 8 bitini temsil eder. Bu sayısal değer anahtar dizesinin her bir karakterinden elde edilen sayısal değer kadar döndürme işlemine tutulur.
4) Döndürme işleminin kaç kez yapılacağı anahtar dizesindeki her bir karakterin sayısal değerinin 64 ile bölünmesinden kalan değer ile belirlenir.
5) Döndürme işleminden sonra elde edilen veri ile 64 bitlik sayısal değere atanan anahtar arasında XOR işlemi gerçekleştirilir.
6) Şifrelenmiş sayısal değer onaltılık sayı tabanında string dizesine dönüştürülür. Dönüştürme işlemi sonrası şifreli blok elde edilmiş olur.
7) Diğer 8 karakterlik bloklar için aynı işlemler tekrar edilir.
8) Son kalan blok 8 karakterden daha az ise gerektiği kadar "*" karakteri yerleştirilerek 8 karaktere tamamlanır.



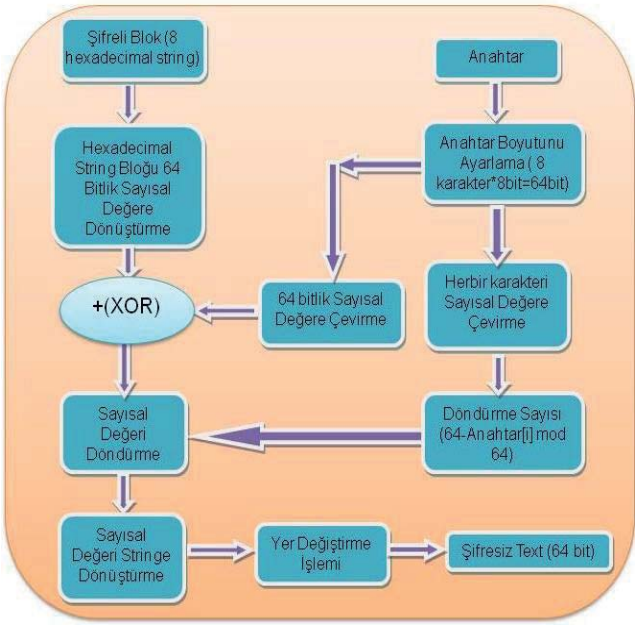
Şekil 2.Şifreleme algoritması akış diyagramı

B. *Şifre Çözme Algoritması*

Çalışmanın bu bölümünde ise geliştirilen algoritmada uygulanan şifre çözme adımları ele alınmış olup şifre çözme algoritması Şekil 3'de akış diyagramı olarak sunulmuştur.

1) Şifre çözme algoritması şifreleme algoritmasında izlenen yolun tersidir. Her bir onaltılık sistemdeki 8 değer blok olarak alınıp, 64 bitlik sayısal değere dönüştürülerek bit seviyesinde çeşitli fonksiyonlardan geçirilir.

2) Şifre çözme işlemine gelen 16 karakter (onaltılık sistemdeki 8 değer) 64 bitlik sayısal değere dönüştürülür.
3) Elde edilen sayısal değer ile 64 bitlik sayısal değere atanan anahtar arasında XOR işlemi gerçekleştirilir. Bu sayısal değer anahtar dizesinin her bir karakterinden elde edilen sayısal değer kadar döndürme işlemine tabi tutulur.
4) Döndürme işleminin kaç kez yapılacağı, anahtar dizesindeki her bir karakterin sayısal değerinin 64 ile bölünmesinden elde edilen kalan değerin, 64 sayısından çıkarılmasıyla belirlenir.
5) Döndürme işlemi sonucu elde edilen sayısal değer stringe dönüştürülür. String dizesi 32 bitlik yer değiştirme işlemine (ilk 4 karakter ve son 4 karakter yer değiştirir) tabi tutularak şifresiz blok elde edilir.
6) Geriye kalan bloklar için de aynı işlemler gerçekleştirilerek şifresiz metin elde edilir.



Şekil 3.Şifre çözme algoritması akış diyagramı

III. E-POSTA PROTOKOLLERİ

POP (Post Office Protokol) protokolü elektronik posta almak için son kullanıcılar tarafından kullanılmaktadır. POP protokolü sayesinde kullanılan e-posta sunucusunda bulunan postalar yerel diske indirilebilmektedir [14].

Elektronik posta gönderme protokolü (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece e-posta göndermek için kullanılan bu protokolde; istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini göndermekte, sunucunun onay vermesi halinde gerekli e-postayı sunucuya iletmekte ve bağlantıyı sonlandırmaktadır [15].

A. Telnet ile POP3 ve SMTP Sunucularına Bağlanma

Herhangi bir e-posta sunucuya bağlanırken normal bir TCP/IP bağlantısı yapılmaktadır. POP3 ile ilgili gerekli ayarları yapmak ve gelen e-postaları almak için gerekli işlemleri yapmak amacıyla telnet kullanılmıştır.

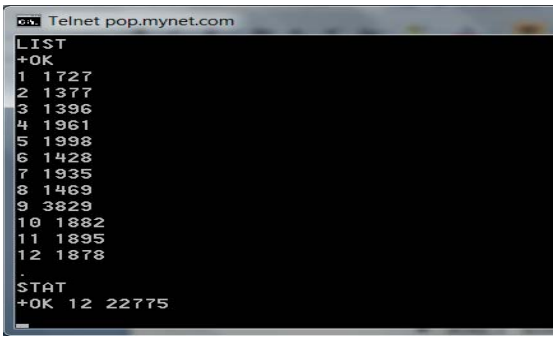
Telnetle bir sunucuya bağlanmak için öncelikle sunucunun adresi ve çalıştığı portu girmek gerekmektedir. Genellikle port için varsayılan değer 110'dur. Bu işlemin sonunda sunucu helo mesajı göndermekte ve bağlantının hazır olduğunu belirtmektedir. Yapılan işlemler doğru olduğu sürece +OK ile cevap alınmaktadır.

Bağlantı sağlandıktan sonra "USER" komutuyla kullanıcı kodu ve "PASS" komutuyla şifre girilerek sunucuya erişim sağlanmaktadır.

Bu aşamadan sonra çalışma sırasında kullanılan önemli komutlar ve görevleri aşağıda belirtilmiştir [16]:

STAT: Gelen kutusunda kaç adet e-posta olduğunu göstermektedir. STAT komutu kullanılarak gelen kutusunda e-posta olup olmadığı ve kaç yeni e-posta geldiğinin kontrolü yapılmıştır (Şekil 4).

LIST: Gelen kutusundaki e-postaların sırasını ve her birinin boyutlarını göstermektedir (Şekil 4).

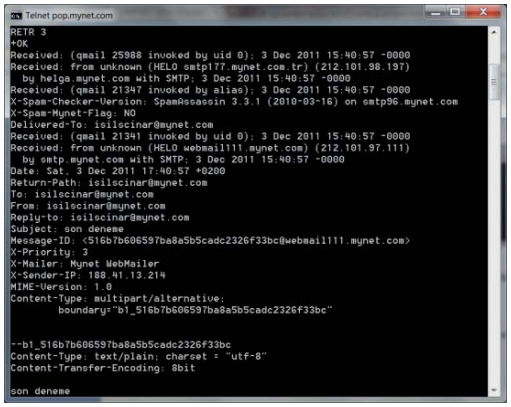


Şekil 4. LIST ve STAT komutlarının çalıştırılması ve örnek sonuçlar

QUIT: POP3 bağlantısını sonlandırmak için kullanılmaktadır.

TOP: E-posta içeriğinin istenilen satıra kadar görülmesini sağlamaktadır. "TOP 2 5" ifadesi, 2 numaralı e-postanın 5.satırına kadar görüntülenmesini sağlamaktadır.

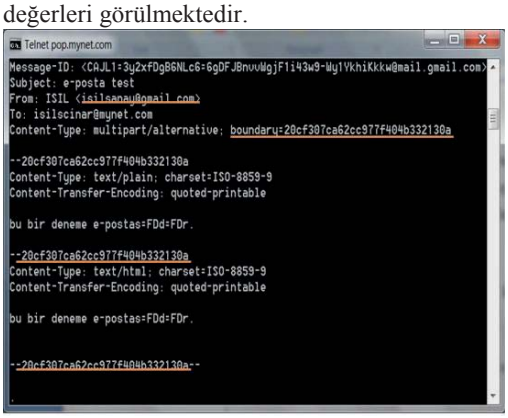
RETR: Bu komutla Şekil 5'te görüldüğü gibi gelen kutusundan istenilen e-postanın sıra numarası yazılarak detaylı olarak içerik bilgileri alınabilmektedir. Buradaki içerik standart e-postaların içeriğine benzememektedir. Buradaki bilgiler e-postanın orjinal halini göstermektedir.



Şekil 5.RETR komutunun çalıştırılması ve örnek sonuçlar

E-posta içeriğinin başlama ve bitişini belirten sınır (Boundary) değeri eğer içerikte varsa string olarak alınır ve

bundan sonraki 2. ve 3. sınır değerleri arasında kalan alan mesajın metninin verildiği alandır. Şekil 6'da Mynet e-posta sunucusuna gönderilen Gmail e-posta içeriği için örnek sınır değerleri görülmektedir.



Şekil 6. Gmail e-posta içeriği için örnek sınır değerleri

Uygulamada SMTP sunucusu olarak Gmail'in e-posta sunucusu kullanılmıştır.

B. *Ücretsiz E-Posta Servis Sağlayıcı İstemci Ayarları*

E-posta işlemleri için kullanılmakta olan Gmail, Yahoo, Mynet, Hotmail gibi ücretsiz e-posta servis sağlayıcılarının bir kısmı SMTP sunucularına erişimi engellerken bir kısmı da POP3 sunucusuna erişimi engellemiş durumdadır. Uygun sunucuların bulunması için TELNET ile bağlantı yapılarak gerekli testlerin yapılması önemlidir.

Tablo 1'de Gmail, Mynet, Yahoo ve Hotmail gibi e-posta hizmet sağlayıcılarının POP3 ve SMTP protokolleri için yapılandırma ayarları yer almaktadır. Yahoo e-posta servisinde POP3 sunucularına erişimi ücretli e-posta hesaplarına sağlamakta iken diğer e-posta servis sağlayıcılar ücretsiz olarak her iki protokolü de hizmete sunmaktadırlar. Ancak servis sağlayıcıların POP3 sunucularından e-posta verilerini alabilmek için web sayfaları üzerindeki e-posta yapılandırma ayarlarından e-posta hesaplarına erişim izninin verilmesi gerekmektedir.

TABLO I
ÜCRETSİZ E-POSTA SERVİSİ SAĞLAYICILARI PROTOKOL YAPILANDIRMA BİLGİLERİ

	Gelen E-Posta Sunucusu(POP3)	POP3 Portu	Giden E-Posta Sunucusu(SMTP)	SMTP Portu
Gmail	pop.gmail.com	995	smtp.gmail.com	587
Mynet	pop.mynet.com	110	pop.mynet.com	587
Yahoo	Yalnızca Ücretli Hesaplara Açık	-	smtp.mail.yahoo.com	587
Hotmail	pop3.live.com	995	smtp.live.com	587

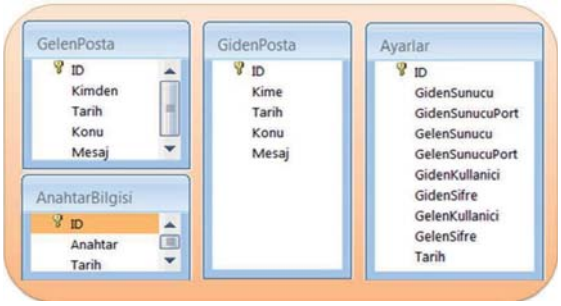
IV. GELİŞTİRİLEN E-POSTA UYGULAMALARI

A. *E-posta Kontrol Uygulaması*

E-posta kontrol uygulaması .NET 2008 platformu üzerinde C# programlama dili ile geliştirilmiş olup e-posta verilerinin tutulacağı veritabanı için MS Access 2007 kullanılmıştır.

Uygulamada temel e-posta gönderme ve alma işlemleri önceki bölümde bahsedilmiş olan Telnet komutları kullanılarak gerçekleştirilmiştir.

Veritabanında bulunan Gelen/Giden e-posta bilgilerinin tutulduğu tablolar, şifreleme işlemi için kullanılan anahtarların tutulduğu AnahtarBilgisi tablosu ve e-posta gönderme/alma işlemlerinde kullanılan sunucu ayarlarının tutulduğu Ayarlar tablosu en basit şekilde Şekil 7'de görülmektedir.



Şekil 7. E-posta kontrol uygulaması veritabanı şeması

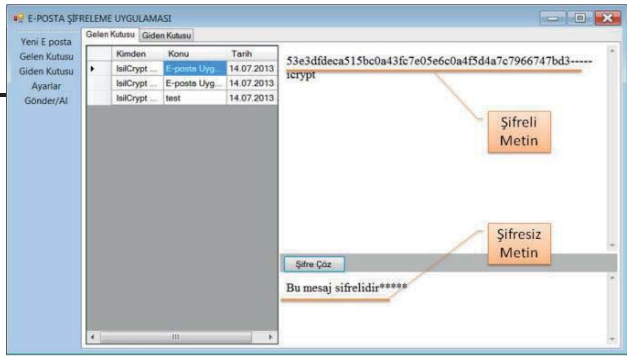
POP3 sunucusundan çekilen e-postalarla ilgili bilgiler gerekli düzenlemelerden geçirilip parçalandıktan sonra gelen posta tablosuna kaydedilmiştir.

Giden e-posta tablosunda uygulamadan gönderilen postaların bilgileri, anahtar bilgisi tablosunda şifreleme algoritmasında kullanılacak anahtar ve anahtarın kaydedildiği tarih bilgisi, ayarlar tablosunda posta gönderme ve alma işlemleri için kullanılan sunucuların bilgileri ve sunucularda yetkili olacak kullanıcının hesap bilgileri ve tarih bilgisi yer almaktadır.

Temel E-Posta İşlemlerinin Gerçekleştirilmesi

Yeni e-posta göndermek için Şekil 8'deki ana menüde "Yeni e-posta" seçeneği seçilerek e-postanın isteğe göre şifrelenmeden veya şifrelenerek gönderilebilmesi sağlanmaktadır. Şifrelenmiş olan e-postaların sonuna uygulamaya özgü bir ifade olan "-----icrypt" ifadesi eklenmektedir.

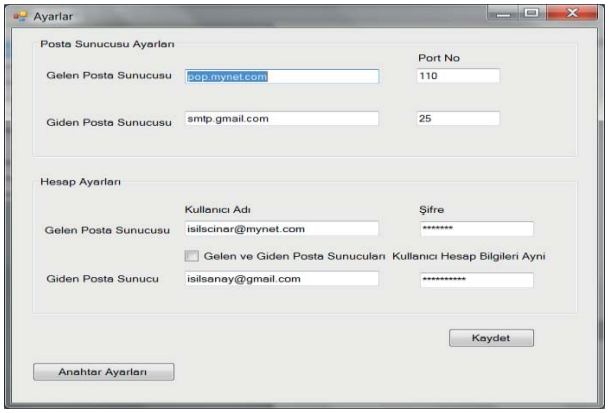
Uygulama gelen e-postanın şifreli veya şifrelenmeden gelmiş olma durumlarını şifrelenmiş olan mesajların sonunda "-----icrypt" ifadesinin bulunup bulunmadığını kontrol ederek yapmaktadır. Böylece e-postanın uygulama içerisindeki algoritmayla şifrelenip şifrelenmediği test edilmektedir. Eğer e-posta şifrelenerek gönderilmişse e-posta alanının altındaki "şifre çöz" butonuna tıklandığında aşağıdaki bölmeye şifrelenmiş mesajın şifresi çözülmüş, orjinal hali yüklenmektedir.



Şekil 8.E-Posta kontrol uygulaması gelen e-posta kutusu

Konfigürasyon İşlemleri

Uygulama içerisindeki ayarlar penceresinden e-posta sunucusu ayarları yapılmaktadır. Bu ayarlar, POP3 sunucusuna bağlanmak için gerekli olan gelen posta sunucusu, port numarası ve SMTP sunucusuna bağlanmak için gerekli olan giden posta sunucusu, port numarası ve her iki sunucu için de kullanıcı hesabı bilgilerini kapsamaktadır. Şekil 9'da örnek konfigürasyon bilgileri sunulmaktadır.



Şekil 9. E-Posta kontrol uygulaması e-posta sunucu, hesap ve anahtar ayarları

Anahtar Ayarları

Anahtar dağıtım sorunu iletişimde bulunan iki tarafın ortak bir şifreleme anahtarı üzerinde anlaşmaları sorunudur. Şifreleme anahtarı ile şifreyi çözme anahtarının aynı olduğu klasik şifreleme algoritmaları kullanan sistemlerde, anahtar dağıtım sorunu ya önceden elden ele anahtarı vererek, ya özel ve güvenli bir kanal vasıtasıyla, ya da güvenli anahtar dağıtım sunucuları kullanarak çözülmektedir [8].

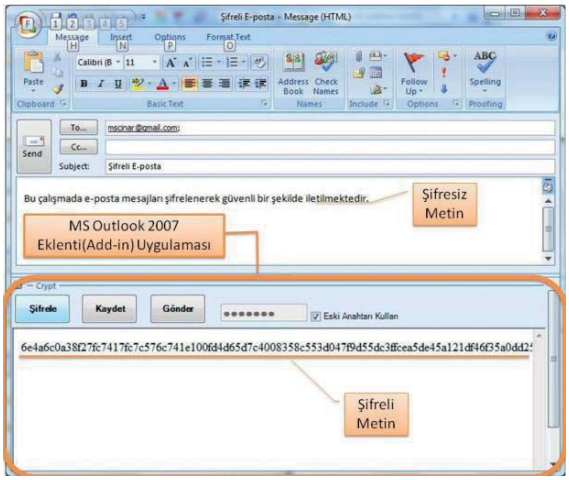
Yapılan çalışmada anahtar paylaşımının özel ve güvenilir bir kanal vasıtasıyla veya güvenli anahtar dağıtım sunucuları kullanılarak gerçekleştirildiği varsayılmıştır. Şifreleme algoritmasında kullanılmış olan ve hem gönderici hem de alıcının bilmesi gereken şifreleme anahtarı Şekil 9'daki anahtar ayarları bağlantısından sisteme kaydedilmektedir.

B. MS Outlook E-Posta Şifreleme Eklenti Uygulaması

Bu çalışma kapsamında geliştirilen ikinci uygulama, MS Outlook programına eklenti olarak (add-in) .NET 2008 platformu üzerinde C# programlama dili ile geliştirilmiştir.

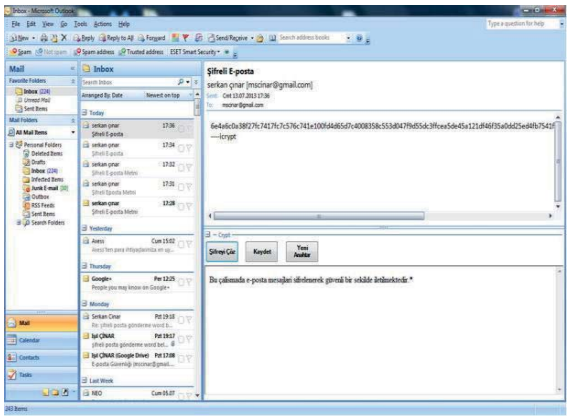
Eklenti uygulamaları programların yeteneklerini artırmak için geliştirilen ve programlara entegre edilebilen küçük programcıklardır [17].

Geliştirilen eklenti uygulaması ile şifreli e-posta gönderme ve alma işlemleri başarılı bir şekilde gerçekleştirilmiştir. Şekil 10'da şifreli e-posta gönderimine ilişkin MS Outlook programının ekran görüntüsü sunulmaktadır.



Şekil 10. MS Outlook 2007 eklentisi şifreli e-posta gönderme ekranı

Şekil 11'de ise gelen şifreli e-postanın geliştirilen outlook eklentisi ile çözülmesi işlemi gösterilmektedir.



Şekil 11. MS Outlook 2007 eklentisi gelen kutusu şifre çözme ekranı

V. GELECEKTE YAPILACAK ÇALIŞMALAR

Gerçekleştirilecek sonraki çalışmalarda, e-posta kontrol uygulaması ve MS Outlook e-posta şifreleme eklenti uygulamasında, e-posta içeriklerinde yer alan farklı türlerdeki dosya eklerinin hızlı ve etkin şifrelenmesi için tasarlanan algoritmanın geliştirilmesi planlanmaktadır. Algoritma, şifrelemede uygulanan; blok bazında yer değiştirme, bit bazında döndürme ve anahtar değeri ile şifreleme fonksiyonundan geçirme işlemleri ile şifre kırma saldırılarına karşı dirençli olmasına rağmen, tüm anahtarların denendiği kaba kuvvet (brute force) saldırılarında, gerekli hesaplama gücü anahtarın uzunluğu ile doğru orantılı olarak artacağından şifrenin kırılmaya karşı güçlendirilmesi için sonraki çalışmalarda anahtar boyutu arttırılarak şifreleme 128 ve 256 bit olarak gerçekleştirilecektir.

Ayrıca çalışmada tasarlanan şifreleme algoritması asimetrik şifreleme algoritmaları ile güçlendirilerek hibrid bir şifreleme algoritması geliştirilmesi planlanmaktadır. Geliştirilecek hibrid algoritma ile anahtar paylaşımında kullanılan açık anahtar altyapıları çalışmada yer alan uygulamalara entegre edilebilecektir.

VI. SONUÇ VE KAZANIMLAR

Bu çalışmayla her geçen gün daha da yaygınlaşmakta olan e-posta kullanımının daha güvenilir olması sağlanmıştır. Çalışmada bilinen yaygın kullanılan şifreleme algoritmaları dışında yeni bir algoritma geliştirilmiştir. DES, AES ve Blowfish gibi simetrik şifreleme algoritmaları yaygın kullanılan ve bilinen algoritmalar olması sebebiyle internet ortamında bu algoritmaların kırılmalarına yönelik çeşitli araçlar ve çalışmalar bulunmaktadır. Bu çalışmada geliştirilen şifreleme algoritmasının özgün olması, en azından programlama bilgisi olmadan hazır araçları kullanarak zaman zaman şifre kırma konusunda başarılı olan kötü niyetli kişilerin hedefi olmaktan kurtarmaktadır.

Uygulama şifreleme özelliği sayesinde güvenlik konusunda getireceği avantajlara ek olarak, ücretsiz e-posta servis sağlayıcılarının izin verdiği ölçüde sunuculara erişmekte ve yapılan konfigürasyonlara göre istenilen hesabın tüm e-postalarını uygulama kendi veritabanına yükleyebilmektedir.

Gmail, Yahoo, Hotmail gibi ücretsiz e-posta servis sağlayıcıların kullanım sözleşmesinde belirttiği üzere; kullanıcı e-postaları bu servis sağlayıcılar tarafından istenildiğinde silinebilmekte veya üçüncü kişilerle paylaşılabilmektedir. Bu çalışma sayesinde e-postalar servis sağlayıcılar tarafından silinme durumuna karşın koruma altına alınmış olmaktadır. Ayrıca e-postalar istenildiğinde şifrelenerek gönderme işlemine tabi tutulduğu için bilgiler üçüncü kişilerin eline geçse dahi gönderilen e-posta içeriği anlaşılmamaktadır.

REFERANSLAR

[1] D. Choukse, U.K. Singh, L. Laddhani ve R. Shahapurkar, "Designing secure email infrastructure," *Wireless and Optical Communications Networks (WOCN)*, 1964, pp. 1–9, 2012.

[2] Ş. Bayzan, "E-Posta Güvenliği Neden Önemlidir?", http://www.guvenliweb.org.tr/guvenlik/node/40, (Erişim: 08.07.2013).

[3] A.M.M.Rao, "Policy Specification and Enforcement for Detection of Security Violations in a Mail Service ," *9th International Conference on Information Technology* , pp. 172–175, 2006.

[4] A. Ghafoor, S. Muftic ve G. Schmölzer," CryptoNET: Design and implementation of the Secure Email System", *2009 Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN)*, pp. 1–6, 2009.

[5] S.J. Stolfo, S. Hershkop, Ke Wang ve O. Nimeskern," EMT/MET: systems for modeling and detecting errant email", *DARPA Information Survivability Conference and Exposition*, vol. 2, pp. 290–295, 2003.

[6] M. Takesue, "E-mail Sender Identification through Trusted Local Deposit-Agents", *IEEE Conf, 2011 14th International Conference on Network-Based Information Systems (NBiS)*, pp. 84–91, 2011.

[7] G.Bahadur, Chan ve W.Weber, "Privacy Defended: Protecting Yourself Online", *Que, Chapter 8*, 2002.

[8] A. Levi ve M.U. Caglayan, "Elektronik Posta Güvenliği ve Açık Anahtar Sunucuları", *Bilişim 97, TBD 14. Bilişim Kurultayı*, pp. 114-117, 1997.

[9] D. Zissis, ve D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, pp.583-592, 2012.

[10] TropSoft,"DES Overview", http://www.tropsoft.com/strongenc/des.htm. Erişim: 01.06.2013.

[11] A. Nadeem, "A Performance Comparison of Data Encryption Algorithms", *IEEE*, 2005.

[12] J. Thakur, ve K. Nagesh, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis.", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 1, pp. 6-12, 2011.

[13] Vikipedi, "Gizli Anahtarlı Şifreleme", http://tr.wikipedia.org/wiki/Gizli_anahtarl%C4%B1_%C5%9Fifreleme, (Erişim: 08.05.2013).

[14] R. Sureswaran ve ark., "Active E-mail system protocols monitoring algorithm", *TENCON 2009 - 2009 IEEE Region 10 Conference*, 2010.

[15] Vikipedi, http://tr.wikipedia.org/wiki/SMTP, Erişim: 12.06.2013.

[16] ProgramlamaTv, "Telnet ile Pop3 Sunucuya Bağlanma ve Mail İşlemleri", http://www.programlamatv.com/ders/bilisim/telnet-ile-pop3-sunucuya-baglanma-ve-mail-islemleri/, (Erişim: 08.07.2012).

[17] J. Boyce, B. Sheresh ve D. Sheresh, "Microsoft® Office Outlook® 2007", *O'Reilly Media, Inc*., 2009.

Muhammet Serkan Çinar, 2011 yılında Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği bölümünden yüksek lisans derecesi almıştır. Şu anda Hacettepe Üniversitesi Bilgisayar Mühendisliği bölümünde doktora öğrencisidir. IPTV tabanlı uzaktan eğitim, yazılım mühendisliği, bilişim güvenliği ve semantik web alanlarında çalışmalar yapmaktadır.

Işıl Çinar, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde yüksek lisans yapmaktadır. Bilişim güvenliği, veri madenciliği, insan bilgisayar etkileşimi alanlarına ilgi duymaktadır.

Hasan Şakir Bilge, 1992 yılında Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği bölümünden mezun oldu. 1997 yılında Kırıkkale Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda yüksek lisansını, 2003 yılında Başkent Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda doktorasını tamamladı. Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde 2003 yılında yardımcı doçent unvanını ve 2012 yılında doçent unvanını aldı.