# RSA Şifreleme Algoritması Kullanılarak SMS İle Güvenli Mesajlaşma Yöntemi

**Hüseyin Bodur[1], Resul Kara[1], Sultan Zavrak[1]**

[1] Düzce Üniversitesi, Bilgisayar Mühendisliği Bölümü, Düzce

huseyinbodur@duzce.edu.tr, resulkara@duzce.edu.tr, sultanzavrak@duzce.edu.tr

**Özet:** İletişim teknolojilerinin hızla gelişmesi, bir yandan birçok teknolojik kolaylığı beraberinde getirip hayatımızı kolaylaştırırken, diğer yandan da çeşitli haberleşme ortamlarında gönderici ve alıcı arasında sürekli dolaşmakta olan bilgilerin gizlenmesi ve üçüncü kişilerle paylaşılmaması konusunda dezavantajlara sahiptir. Belirli güvenlik metotları ve algoritmaları ile bu dezavantajların ortadan kaldırılmasının hedeflenmesi ise kriptoloji adı verilen, bilgi güvenliğini içeren bilim dalının konusudur.

Bu çalışmada, Android işletim sistemine sahip cihazlarda, RSA şifreleme algoritması ile SMS kanalı üzerinde güvenli mesajlaşma işleminin nasıl gerçekleştirildiği geliştirilen uygulama üzerinde incelenmekte, avantaj ve dezavantajları ortaya konulmakta ve çözüm önerilerinde bulunulmaktadır.

**Anahtar Sözcükler:** Kriptoloji, RSA Şifreleme, SMS, Güvenli Haberleşme.

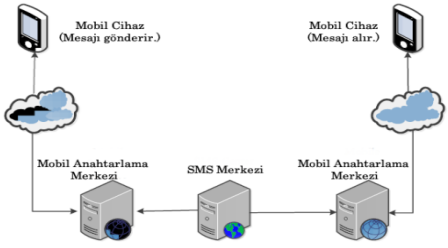
**Secure Messaging Method With SMS Using RSA Encryption Algorithm**

**Abstract:** The rapid development of communication technology, on the one hand, is bringing many technological conveniences with it and simplifying our lives. On the other hand it has disadvantages on hiding the information that is continuously roaming through various communication media resources between senders and receivers and on not sharing them with third people.
The aim of eliminating these disadvantages via specific security methods and algorithms is related to the discipline called cryptography, which includes information security.
In this study, how RSA encryption algorithm and the secure messaging process on the SMS channel are realized in the devices with the Android operating system is examined thanks to the improved application, and the advantages and the disadvantages of the application are demonstrated, and solution proposals are presented.

**Keywords:** Cryptology , RSA Encryption, SMS Encryption, Secure Communication.

## 1. Giriş

Günümüz iletişim teknolojisinde güvenlik konusu önemli bir yer tutmaktadır.
Karşılıklı haberleşmenin üçüncü kişilerin müdahalesine geçit vermeyen güvenli kanallar aracılığıyla yapılması gerektiğinden bu kanalların güvenlik seviyelerinin mümkün olduğunca yüksek tutulması büyük bir önem arz etmektedir.
Karşılıklı haberleşme; konuşma, mesajlaşma vb. yollar ile sağlanmakta, bu yollardan gerçekleştirilen haberleşme işlemi sırasında kullanıcıya fark ettirmeden çeşitli güvenlik metotları, servis sağlayıcı firmalar yâda yazılım firmaları tarafından uygulanabilmektedir.
Güvenlik metotları arasında şifreleme algoritmaları ise büyük bir öneme sahiptir. Bu algoritmalar karmaşıklıklarına göre sıralanmakta, karşılıklı iletişime sızabilecek üçüncü kişiler tarafından ele geçirildiği andan itibaren kendi karmaşıklığı ve gücü oranında direnmektedir.
Mobil iletişimdeki hızlı gelişmeler sonucunda, hem iş dünyasında hem de sosyal ortamlarda SMS ile haberleşme yaygın bir şekilde kullanılmaktadır. 160 karaktere kadar izin verilen SMS mesajlarının, her bir karakteri 7 bit ile oluşturulursa [1] toplamda 1120 bit ile insanlar, kendi özel konularını, işleriyle yâda sosyal ilişkileriyle ilgili olan bilgilerini kolay ve hızlı bir şekilde paylaşabilir hale geldiler [2]. Şekil 1'de SMS ile mesajlaşma yönteminin mimari yapısına dikkat edilirse, SMS'lerin göndericiden alıcıya hiçbir zaman doğrudan teslim edilmediği görülür.




**Şekil 1.** SMS mimarisi

Gönderilen SMS öncelikle mesaj yönlendirme işlemini gerçekleştiren Mobil anahtarlama merkezinden geçer. Ardından SMS merkezinde depolanır ve buradan iletim işlemi için yönlendirilir [3].
Mesajlar mobil anahtarlama istasyonları ve SMS merkezleri arasında açık metin olarak iletilir. Yani iletim sırasında hiçbir şifreleme yâda gizleme işlemine tabi tutulmazlar. Bu durum ise bir takım dezavantajlar meydana getirir.
Bu dezavantajlar şöyle sıralanabilir;

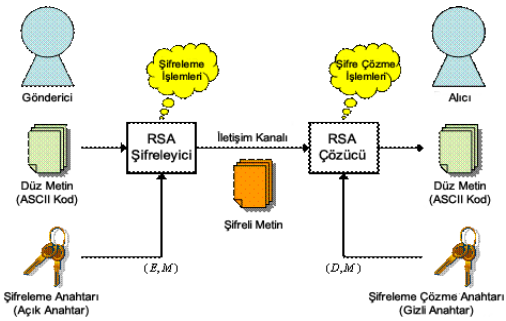
- Mesaj içeriği göndericiden alıcıya ulaşmadan önce, açık metin olarak ilgili operatörün sisteminde saklanır.
- Mesaj içeriği operatör personeli tarafından okunabilir.
- Mesaj içeriklerini tutan operatör sisteminin dış tehditlere karşı ne kadar güvenilir olduğu belirsizdir.
- Mesaj içerikleri, gereken durumlarda mahkemeler tarafından ilgili operatörlerden istenildiği takdirde rahatlıkla ortaya çıkarılabilir.

Bu gibi durumların ortadan kaldırılabilmesi ve güvenli mesajlaşma ortamının sağlanabilmesi için şifreleme algoritmalarından yararlanılabilir. Bu sayede iletim ortamında mesajların açık metin hali değil şifreli hali dolaşacaktır. Şifreli veriyi ele geçiren kişi gerekli metoda yâda anahtara sahip olmadığı müddetçe şifreli halinden orijinal mesajı elde edemeyecektir.
Şifreleme yöntemleri gizli anahtarlı ve açık anahtarlı olmak üzere iki kategoriye ayrılır.
Gizli anahtarlı şifrelemede mesajı şifreleyen göndericinin kullandığı şifreleme anahtarı, mesajı çözecek olan alıcının kullandığı şifreleme anahtarı ile aynıdır. Bu durumda iletilen şifreli mesajın haricinde, şifreleme anahtarının da gizli bir şekilde iletilmesi gerekir ki bu durum gizli anahtarlı şifreleme [4] yönteminin dezavantajlarından bir tanesidir. Ortamı dinleyen yâda operatör sistemine girmeyi başaran üçüncü bir kişi

anahtar değerini ele geçirdiği takdirde şifreli veriyi orijinal haline çevirebilir.
Diğer yöntem olan açık anahtarlı şifrelemenin en önemli özelliği, mesajı şifreleyen anahtar ile çözen anahtar değerinin birbirinden farklı olmasıdır. Bu yöntemde her kullanıcının özel ve açık olmak üzere iki anahtarı vardır. Kullanıcının açık anahtarı herkes tarafından görüntülenebilir. Gizli anahtar ise kullanıcı tarafından gizli tutulur. Kullanıcıya bir mesaj gönderilmek istendiğinde, kullanıcının açık anahtarı kullanılıp mesaj şifreli hale getirilir ve şifreli veri kullanıcıya gönderilir. Kullanıcı şifreli veriyi kendi gizli anahtarı ile çözer ve anlamlı mesajı elde eder. Kullanıcının açık anahtarı ile şifrelenmiş veriyi sadece kullanıcının gizli anahtarı çözebilir [4].
Kullanıcı bir mesaj göndermek istediğinde, açık anahtar kütüphanesine gider. Mesajı göndermek istediği kişinin açık anahtarını alır ve mesajı şifreleyip alıcıya gönderir. Alıcının yapması gereken tek şey kendi gizli anahtarı ile kendisine gelen mesajı çözmek olacaktır.
Bu çalışmada, SMS ile güvenli mesajlaşma işlemi için gizli anahtarlı şifreleme algoritmalarına göre daha güvenilir olan, açık anahtarlı şifreleme yöntemini kullanan algoritmalar arasından RSA algoritması kullanılmıştır.

## 2. RSA Algoritması

RSA şifreleme algoritması, dijital ortamda verilerin güvenli aktarımının sağlanması fikri temel alınarak, tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür açık anahtarlı şifreleme yöntemidir [5]. Günümüzde en çok kullanılan hem şifreleme hem de sayısal imza atma olanağı tanıyan yöntem olarak bilinir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından ortaya çıkarılmıştır.
RSA şifreleme yönteminde, anahtar oluşturma işlemi için asal sayılar kullanılır. Bu da daha güvenli bir yapı oluşturulmasını sağlar. Şekil 2'de RSA algoritmasında şifreleme ve şifre çözme işlemlerinin nasıl yapıldığı gösterilmiştir.




**Şekil 2.** RSA algoritma yapısı

### 2.1 Algoritmanın Yapısı

- P ve Q gibi çok büyük iki asal sayı seçilir.
- Bu iki asal sayının çarpımı N = P.Q ve birer eksiklerinin φ(N)=(P-1)(Q-1) değeri hesaplanır.
- 1'den büyük φ(N)'den küçük φ(N) ile aralarında asal bir M tamsayısı seçilir.
- Gizli üs D, seçilen M tamsayısının mod φ(N)'de tersi alınarak elde edilir.
- M ve N tamsayıları açık anahtarı, D ve N tamsayıları ise gizli anahtarı oluşturur. P, Q ve φ(N) değerleri de gizli anahtar gibi gizli tutulmalıdır.

Açık ve gizli anahtarları oluşturduktan sonra gönderilmek istenen bilgi genel anahtar ile şifrelenir. Şifreleme işlemi şu şekilde yapılmaktadır: Şifrelenecek bilginin sayısal karşılığının M' ninci kuvveti alınır ve bunun mod N deki karşılığı şifrelenmiş metni oluşturur.
Açık anahtar ile şifrelenmiş bir metin ancak gizli anahtar ile açılabilir. Bu yüzden şifrelenmiş metin, yine aynı yolla, şifrelenmiş metnin sayısal karşılığının D' inci kuvveti alınıp, bunun mod N deki karşılığı bulunarak orijinal metne çevrilebilir.

## 3. Yöntem

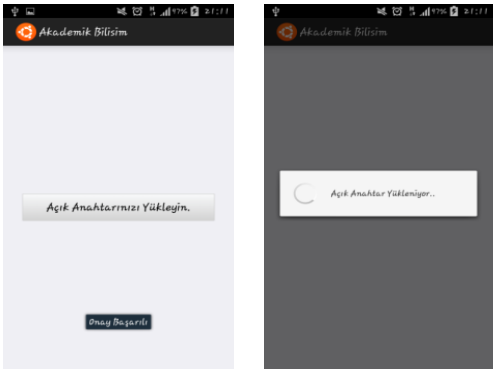
RSA şifreleme algoritmasının Android tabanlı mobil cihazlar üzerinde SMS ile mesaj gönderme işleminde kullanılması için Java platformu üzerinde bir uygulama

geliştirilmiştir. SMS ile mesajlaşmada şifreleme algoritmalarının uygulandığı benzer çalışmalar mevcuttur. Bu çalışmalardan birinde gizli anahtarlı (simetrik) şifreleme algoritmaları olan AES ve 3D-AES ile şifreleme metotları yazılmış ve bu metotların performansları karşılaştırılmıştır. Karşılaştırma sonucunda şifrelenecek açık metnin uzunluğu 0-256 bit aralığında iken AES algoritmasının, 256 bit ve üzeri durumlarda ise 3D-AES algoritmasının performansının daha yüksek olduğu vurgulanmıştır [3].

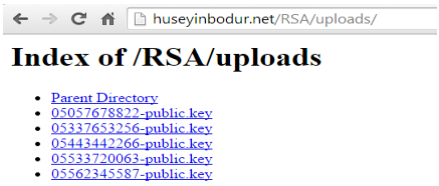
Diğer bir çalışmada ise gizli ve açık anahtarlı (asimetrik) şifreleme yöntemlerinin birbirlerine göre üstünlükleri irdelenmiş, ardından iki açık anahtarlı şifreleme algoritması olan RSA ve ECDH algoritmalarının performans ve güvenlik alanlarında karşılaştırılması ve analizi hedef alınmıştır [6].

Bu ve buna benzer çalışmalardan elde edilen sonuç, açık anahtarlı sistemlerin güvenlik seviyelerinin, gizli anahtarlı sistemlere göre daha yüksek olduğudur.

Şekil 3 ve Şekil 4'te görüleceği üzere, geliştirilen uygulamada her kullanıcının RSA algoritması ile şifreleme işlemine başlamadan açık ve gizli anahtarını belirlemesi ve açık anahtarını, anahtar kütüphanesine yüklemesi gerekir. Açık anahtar adı olarak kullanıcının telefon numara bilgisini kullanmak, hangi açık anahtarın hangi kullanıcıya ait olduğunu tespit etmek konusunda kolaylık sağlayacaktır.

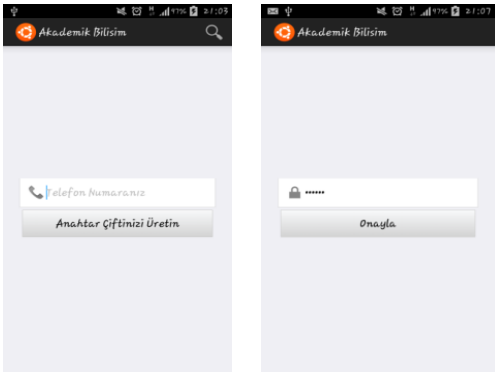



**Şekil 3.** Anahtar çiftleri üretme ve açık anahtarı kütüphaneye yükleme



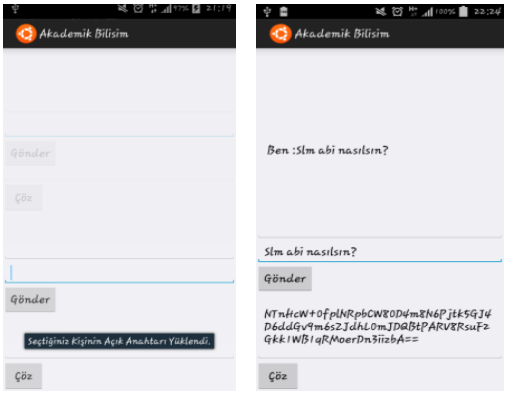

**Şekil 4.** Anahtar kütüphanesinde yüklü olan açık anahtarlar.

Açık ve gizli anahtar bir sefere mahsus oluşturulur. Uygulama, kullanıcıdan bir daha bu iki anahtar değerini oluşturmasını ve açık anahtarını anahtar kütüphanesine yüklemesini istemez. Açık anahtar yüklendikten sonra kullanıcı rehber üzerinde mesaj göndermek istediği bir kişiyi seçer (Şekil 5).



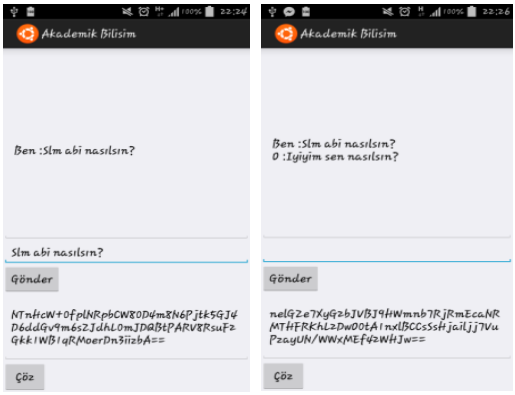

**Şekil 5.** Kullanıcı rehberi

Eğer o kişi de uygulamayı kullanıyorsa (açık anahtarı kütüphanede yüklü ise), kişinin açık anahtarı kütüphaneden alınır ve kullanıcı mesaj göndereceği sayfaya yönlendirilir. Bu sayfa aracılığıyla mesajını yazar ve gönderir (Şekil 6). Mesaj karşı tarafa ulaştığında karşı tarafın yapması gereken tek işlem uygulamayı açıp şifreli veriyi içerik alanına taşımak ve çöz butonuna basmaktır. Kullanıcının mesajlaşmak istediği kişinin açık anahtarı kütüphanede yüklü değilse bu, karşı tarafın uygulamayı kullanmadığı anlamına gelir.



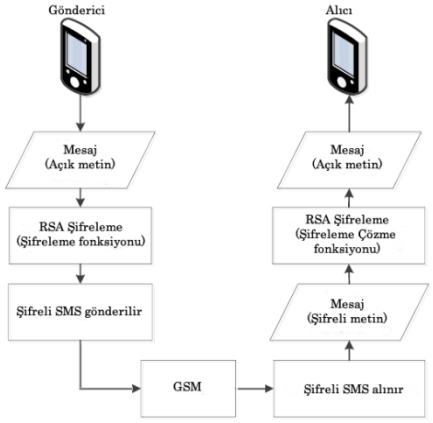

**Şekil 6.** Karşı tarafın açık anahtarının yüklenmesi ve şifreli mesajlaşma başlangıcı

Şekil 7'deki sayfada şifreli mesaj içeriğinin görüntülenmesi için basit bir ekran tasarımı yapılmıştır. Kullanıcı kendi açık anahtarını anahtar kütüphanesine yükleyip, mesajlaşmak istediği kişinin açık anahtarını kendi sistemine dâhil ettikten sonra, uygulamanın bir sonraki mesajlaşmaları için yeniden internet üzerinden anahtar paketleri alıp göndermesine gerek yoktur. İnternet sadece ilk eşleme dönemi için gereklidir.
Uygulama ilklendirme işlemleri tamamlandıktan sonra taraflar karşılıklı mesajlaşmaya başlayabilir.




**Şekil 7.** Şifreli mesajlaşma

Uygulanan şifreleme işlemlerinin genel yapısı Şekil 8'deki gibidir.




**Şekil 8.** Şifreli SMS gönderme genel yapısı

## 4.Yöntemin Test Edilmesi ve Analiz Sonuçları

Mesajın şifreli halinin SMS kanalıyla gönderilmesinde sorun yaşanmaması için, ikili verilerin sadece ASCII karakterlerini kullanan ortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şeması olan Base64 yapısı ile şifrelenmesi gerekir.
Base64 sınıfı mesajın şifreli haline bir standart getirir. Bu standarda göre belli bir blok karakter sayısını geçmediği takdirde

mesajın içeriği kaç karakter olursa olsun, şifrelenmiş hali aynı uzunluktadır.
Mesela tablo 4.1'e bakacak olursak, 512 bitlik anahtar değeri için şifrelenecek mesaj uzunluğu 0-64 karakter aralığındadır. Bunun nedeni 512 bitin (her karakter 8 bit), 64 karakter uzunluğuna eşdeğer olmasıdır. Yani 512 bitlik bir RSA anahtarının şifreleyeceği mesajın maksimum karakter uzunluğu 64'dür. Eğer mesajın içeriği 64 karakterden fazla ise yapılması gereken açık metni bloklara ayırmaktır. 0 - 64 karakter aralığındaki bir mesajdan elde edilecek şifreli veri uzunluğu ise 88 karakter olacaktır.
Anahtar boyutu 1024 olduğunda, 0-128 karakter aralığında metin şifrelenebilir ve şifreli metnin boyutu 172 karakter uzunluğundadır.
Anahtar boyutu 2048 olduğunda ise, 0-256 karakter aralığında metin şifrelenebilir ve şifreli metnin boyutu 344 karakter uzunluğundadır. Diğer anahtar boyutları için mesaj ve şifre uzunlukları Tablo 1'de verilmiştir.

**Tablo 1.** Farklı anahtar boyutlarında en fazla gönderilebilecek mesaj uzunlukları

| Boyut | Mesaj Uzunluğu | Şifre Uzunluğu |
|---|---|---|
| 256 bit | 0-32 karakter | 44 karakter |
| 512 bit | 0-64 karakter | 88 karakter |
| 1024 bit | 0-128 karakter | 172 karakter |
| 2048 bit | 0-256 karakter | 344 karakter |
| 3072 bit | 0-384 karakter | 512 karakter |
| 4096 bit | 0-512 karakter | 684 karakter |
| 8192 bit | 0-1024 karakter | 1368 karakter |

Dikkat edilmesi gereken bir diğer husus ise, SMS mesajlaşma hizmeti ile maksimum kaç karakterli bir veri gönderileceğidir.
Hiçbir şifreleme algoritmasına tabi tutulmayan açık metin halinde bir mesajın, 1120 bit yani 160 karakter seviyesine [1] kadar iletimi mümkündür. Tablo 1 incelendiğinde, bir mesajın 1024 veya 2048 bitlik anahtar boyutları kullanıldığında, şifreli verinin 172 ve 344 karakterden oluşacağı görülür. Bu durumda herhangi bir sıkıştırma algoritması kullanılmadığı takdirde SMS şifreleme üzerinde 1024 yâda 2048 bitlik anahtar değerlerine sahip bir RSA anahtarı ile şifreleme yapmak SMS mesajı iletimi açısından uygun değildir.
512 bitlik RSA anahtar değeri için ise, şifreli mesaj 88 karakter olacağından, anahtar boyutu olarak 512 biti seçmek daha doğru olacaktır. Bu durumun dezavantajı, anahtar boyutu 512 bit yani 64 karakter olduğundan tek blokluk mesaj için en fazla 64 karaktere kadar mesaj iletimi yapabilmesidir.
Bu dezavantajı gidermenin iki yolu vardır. Birincisi mesajın şifrelenmeden önce maksimum 64 karakter olacak şekilde bloklara ayrılmasıdır. Bu ayırma işlemi için, mesajın kaç bloğa bölünmesi gerektiği yalancı kod olarak Şekil 9'da verilmiştir.

512 bit anahtar boyutu için;

$$If\ (mesaj\_boyutu > 64\ and\ mesaj\_boyutu\ mod\ 64 = 0)$$
$$blok\_sayisi = mesaj\_boyutu / 64;$$

$$else\ If(mesaj\_boyutu > 64\ and\ mesaj\_boyutu\ mod\ 64 != 0)$$
$$blok\_sayisi = ((tamsayi)mesaj\_boyutu/64) + 1;$$

**Şekil 9.** Blok Sayısı Bulma Yalancı Kodu

İkinci yol ise 1024 yâda 2048 bitlik anahtar boyutlarının kullanılmasıdır. Çünkü anahtar boyutu arttıkça hem güvenlik seviyesi hem de iletilebilecek maksimum karakter sayısı artar. Fakat SMS kısıtlaması 160 karakter ile sabit olduğundan, açık mesaj yâda mesajın şifreli hali üzerinde sıkıştırma işlemi uygulamak gerekir. Farklı anahtar boyutlarının hesaplanma süreleri Tablo 2'de verilmiştir.

**Tablo 2.** Farklı anahtar bitlerinin ortalama oluşturulma süreleri

| Anahtar Boyutu | Milisaniye |
|---|---|
| 256 bit | 27 |
| 512 bit | 84 |
| 1024 bit | 411 |
| 2048 bit | 2041 |
| 3072 bit | 6010 |
| 4096 bit | 14630 |
| 8192 bit | 174115 |

Şifreleme anahtarının uzunluğunun artması

hem güvenlik seviyesinin hem de iletilebilecek karakter sayısının artması bakımından avantajlara sahiptir. Dezavantajı ise bu uzunluğun beraberinde, yapılan şifreleme ve şifre çözme işlemleri için daha fazla matematiksel işlemler gerektirmesi, işlem maliyetini arttırmasıdır.

## 5.Sonuç ve Öneriler

SMS ile haberleşme yönteminde mesaj içeriğinin göndericiden alıcıya doğrudan iletilmemesi, arada birkaç yönlendirici ve merkez yapılarından geçiyor olması ve gönderilen mesajın açık metin halinde bu yapılar arasında dolaşması güvenlik açısından büyük bir dezavantajdır.

Bu dezavantajın ortadan kaldırılabilmesi için şifreleme yapılarını kullanmak doğru bir yaklaşımdır. Bu sayede mesajın güvenlik seviyesi arttırılabilir. Fakat bu noktadaki en büyük çıkmaz SMS ile iletilebilecek mesaj boyutunun sınırlı olmasıdır. Şifreli halinin, orijinal mesajdan daha büyük boyutlarda olması, maksimum karakterde gönderilecek mesajın daha küçük boyutlarda olmasına neden olur.

Bu sorunun çözümü için, güvenlik seviyesine uygun anahtar boyutu seçildikten sonra, anahtar boyutuna karşılık gelen maksimum karakter sayısına göre hem mesaj üzerinde sıkıştırma yapmak hem de mesaj içeriğini bloklara ayırmak en doğru karar olacaktır.

Açık anahtarların internet bağlantılı bir kütüphanede saklanıyor olması, birkaç kez ile sınırlı olsa da cihazın internet bağlantılı olmasını gerektirir. SMS mesajı gönderme işlemi için internet bağlantısı gerekmesi bir diğer dezavantajdır. Bu dezavantaj, mesajlaşmasının tamamıyla internet ortamında yapılması ve SMS gönderiminin aradan çıkartılmasıyla çözülebilir. Bu çözüm aynı zamanda SMS teknolojisinin sınırlı mesaj iletim sorunu için de bir çözümdür.

Şifreleme yöntemi için simetrik algoritmaları kullanmak bir diğer çözüm olabilir. Bu durumda mesajlaşacak iki taraf arasında öncelikle anahtar paylaşımı yapılıp, ardından şifreli mesajlar gönderilebilir. Alıcı taraf kendisine yollanan anahtar ile mesaj içeriğini çözebilir. Burada iki hat arasını dinleyen üçüncü şahıslar yâda kötü niyetli operatör elemanları bu anahtar değerini ve mesajı ele geçirdiği takdirde şifreli veriyi çözebilirler. Bu nedenle tarafların anahtar paylaşımını yüksek güvenlikli ortamlarda yapmaları gerekir.

## 6.Kaynaklar


[1] Peersman, Gert, et al. "A tutorial overview of the short message service within GSM." Computing & Control Engineering Journal 11.2 (2000): 79-89.

[2] Peersman, C., et al. "The global system for mobile communications short message service." Personal Communications, IEEE 7.3 (2000): 15-23.

[3] Ariffi, Suriyani, et al. "SMS Encryption Using 3D-AES Block Cipher on Android Message Application." Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on. IEEE, 2013.

[4] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems. *http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf* Erişim tarihi : 1 Aralık 2014

[5] Rivest R. L., Shamir A. ve Adleman L., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2):120-126, February1978.

[6] Neidhardt, Eric. "Asymmetric Cryptography for Mobile Devices."