[9] https://www.pcmag.com/news/10-best-practices-for-securing-big-data

RSA (RİVEST-SHAMİR-ADLEMAN) ALQORİTMİ VƏ ONUN TƏTBİQİ

İsmayıllı Nəzrin Elşən
"R.İ.S.K. Elmi İstehsalat Şirkəti" Qapalı Səhmdar Cəmiyyəti

Xülasə
Dünya sürətlə rəqəmsal dövrə keçid edir və məlumatların təhlükəsiz ötürülməsi, həmçinin saxlanması vacib hala gəlir. Kriptoqrafiya, bu məqsədə xidmət edən mühüm bir sahədir, hansı ki, məlumatların şifrələnməsi və deşifrə edilməsi üçün istifadə olunur. Kriptoqrafiyanın əsas formalarından biri açıq açarlı (asimmetrik) kriptoqrafiyadır və bu sahədə RSA (Rivest-Shamir-Adleman) alqoritmi önəmli yer tutur. RSA, məlumatların təhlükəsizliyini təmin etmək üçün açıq və gizli açarlardan istifadə edir. Bu alqoritm böyük sadə ədədlərin faktorizasiyasına əsaslanaraq, məlumatların yalnız müvafiq şəxsi açarla deşifrə edilə bilməsini təmin edir. RSA alqoritmi 1978-ci ildə yaradılıb və bu gün müasir kriptoqrafiyada geniş istifadə olunur. Bu məqalədə RSA alqoritminin iş prinsipləri, açarların yaradılması, şifrələmə və deşifrə prosesi ətraflı izah olunur. RSA alqoritmi internet əlaqələrində, elektron poçtlarda, məlumat bazalarında və rəqəmsal imzalarda geniş istifadə edilir. Güclü təhlükəsizlik təmin etməsinə baxmayaraq, uzun açarlar və yavaş işləmə sürəti kimi məhdudiyyətləri var. Bu məqalənin məqsədi RSA alqoritminin əsas prinsiplərini, işləmə mexanizmini və praktiki tətbiq sahələrini oxuculara izah etməkdir. RSA-nın üstünlükləri və çatışmazlıqları haqqında da ətraflı məlumat veriləcəkdir. Nəticə olaraq, RSA alqoritmi müasir rəqəmsal dünyada məlumatların təhlükəsizliyini təmin etmək üçün əhəmiyyətli bir alqoritm olaraq qalır və texnologiyanın inkişafı ilə birlikdə daha da təkmilləşdirilməsi vacibdir.
Açar sözlər – RSA alqoritmi, kriptoqrafiya, şifrələmə, açıq açar, gizli açar, təhlükəsizlik, simmetrik şiifrələmə, asimmetrik şifrələmə

Giriş

Dünya ictimaiyyəti artıq rəqəmsal dünyaya keçid edir. Hər birimiz məlumatların göndəriləcəyi və qəbul ediləcəyi dövriyyəyə aidik. Amma, bu artıq onlayn ictimaiyyətdə, hər bir şəxsin etibarlı olmadığı bir mühitdə, mümkün olur. Bu səbəbdən, məlumatların təhlükəsizliyi çox əhəmiyyətli vəziyyətə gəlir.
Kriptoqrafiya, bu məsələdən məsul olan bir sahədir. Kriptoqrafiya, məlumatları şifrələmə, şifrələnmiş məlumatı deşifrə etmək üçün istifadə olunan texnologiyalardan ibarətdir. Əsas məqsəd, məlumatların gizliliyini, bütövlüyünü və əminliyini təmin etməkdir. Kriptoqrafiya, internet əlaqələrində, bank işlərində, rəqəmsal imzalarda və daha bir çox sahədə istifadə olunur.
Kriptoqrafiyanın iki əsas forması var: simmetrik və açıq açarlı (asimmetrik) kriptoqrafiya. Simmetrik kriptoqrafiyada, eyni açar məlumatı şifrələmək və açmaq üçün istifadə olunur. Asimmetrik kriptoqrafiyada isə, hər bir istifadəçi iki ədəd açar istifadə edir: açıq açar və gizli açar. Açıq açar hər kəs tərəfindən bilinir və məlumatın şifrələnməsi üçün istifadə olunur, lakin yalnız gizli açar, şifrələnmiş məlumatı açmaq üçün istifadə olunur. Bu, açıq açarlı kriptoqrafiyanın əsas prinsipidir və RSA, bu texnologiyaya əsaslanan məşhur bir alqoritmdir.
RSA 1978-ci ildə Ron Rivest, Adi Shamir və Leonard Adleman tərəfindən yaradılmış açıq açarlı kriptoqrafiya alqoritmidir. Bu alqoritmdə, məlumatların şifrələnməsi və açılması üçün iki ədəd açar istifadə olunur: açıq açar və gizli açar. Açıq açar, hər kəs tərəfindən bilinən və məlumatların şifrələnməsi üçün istifadə olunan bir açardır. Məlumatları göndərmək istəyən şəxslər açıq açarı istifadə edir və məlumatı göndərməzdən əvvəl şifrələyir. Gizli açar, tək bir şəxsin biləcəyi gizli bir açardır. Bu açar, məlumatları şifrələmək və şifrələnmiş məlumatı açmaq üçün istifadə olunur.

RSA alqoritmi, böyük sadə ədədlərin faktorizasiya problemi ilə əlaqəlidir. Bu, bir ədədin məhdudiyyətsiz bütün bölmələrinin tapılması və bu bölümlərdən iki ədədin tapılması məsələsidir. RSA, bu problemin həlli üçün böyük sadə ədədləri istifadə edir və bu ədədlərin faktorizasiyasını ənənəvi kompüterlərdə milyonlarla illik müddətdə həll edilə bilməsi səbəbindən təhlükəsiz bir şifrələmə alqoritmi olaraq qalır. RSA, müasir kriptoqrafiya texnologiyasında ən məşhur və yayğın istifadə olunan alqoritmlərdən biridir. İnternet əlaqələrində, elektron poçtlarında, məlumat bazalarında və rəqəmsal imzalarda istifadə olunur. Güclü təhlükəsizlik təmin etməsinə baxmayaraq, uzun açarlar və yavaş işləmə sürəti kimi məhdudiyyətləri var. Bununla birlikdə, RSA, rəqəmsal əlaqələr və məlumatların təhlükəsizliyi üçün əsas bir element kimi qalır. RSA alqoritminin bir sıra üstünlükləri və çatışmazlıqları vardır.

RSA alqoritminin üstünlükləri:

- Təhlükəsizlik: RSA alqoritmi, məlumatların təhlükəsiz ötürülməsini təmin etmək üçün güclü bir alqoritmdir. Şifrələmə və deşifrə prosesləri üçün mürəkkəb riyazi əməliyyatlar tələb edir, bu da təhlükəsizliyi artırır.
- Açıq açar kriptoqrafiyası: RSA, açıq açar kriptoqrafiya üsullarından biri olaraq bilinir. Bu, məlumatları şifrələmək və açmaq üçün fərqli açarların istifadə edilməsini tələb edir. Bu, məlumatların təhlükəsiz bir şəkildə ötürülməsini təmin etməyə kömək edir.
- Açar mübadiləsi: RSA, açar mübadiləsi üçün ideal bir alqoritmdir. İstifadəçilər, məlumatları şifrələmək üçün açıq açarları paylaşa bilər və sonra məlumatları qəbul edən tərəf, məlumatları açmaq üçün öz şəxsi açarını istifadə edər.
- Rəqəmsal imzalar: RSA, rəqəmsal imza funksiyaları üçün də mükəmməldir. Bu, məlumatların təhlükəsizliyini və mənbəyini doğrulamaq üçün istifadə olunur.

RSA alqoritminin çatışmazlıqları:

- Yavaş emal sürəti: RSA alqoritmi, büyük məlumat həcmi ilə işləyərkən digər şifrələmə alqoritmləri ilə müqayisədə yavaş emal sürətinə malikdir. Bu, məlumatları şifrələmə və açmaq proseslərində vaxtın artmasına səbəb olur.
- Böyük açar ölçüsü: RSA, təhlükəsizlik üçün böyük açar ölçülərinin istifadəsini tələb edir. Bu, hesablama gücü və yaddaş səviyyəsində ciddi tələblərə səbəb olur.
- Yan kanal hücumlarına qarşı zəiflik: RSA, yan kanal hücumlarına qarşı zəifdir. Bu, təcavüzkarların açıq açar məlumatını çıxarmaq üçün yan kanallar vasitəsilə sızan məlumatdan istifadə etmələrinə imkan verir.

Nəticədə, RSA alqoritmi, kriptoqrafiyanın ən əsas elementlərindən biri olaraq qalır. Hər nə qədər bəzi çatışmazlıqlar və təhlükəsizlik riskləri olsa da, düzgün tətbiq edildikdə, hələ də effektiv bir şifrələmə alqoritmi olaraq qalır. Bununla birlikdə, texnologiya inkişafı ilə birlikdə, RSA-nın təhlükəsizlik mövzusunda daha da təkmilləşdirilməsi və mövcud risklərin azaldılması üçün davam etmək vacibdir.

Məqsəd

RSA alqoritminin əsas məqsədi, məlumatların təhlükəsizliyini təmin etmək və şifrələnmiş məlumatları yalnız səlahiyyətli şəxslərin oxuya bilməsini təmin etməkdir. Bu alqoritm, iki əsas açar dəstindən – açıq açar və gizli açardan - istifadə edərək, məlumatların şifrələnməsi və deşifrələnməsini təmin edir. Açıq açar hər kəs tərəfindən istifadə oluna bilər, lakin gizli açar yalnız onun sahibi tərəfindən saxlanılır və istifadə olunur. RSA-nın əsas məqsədləri aşağıdakılardır:

- Məlumatın məxfiliyi (Confidentiality): Məlumatın yalnız nəzərdə tutulan alıcı tərəfindən oxuna bilməsini təmin etmək.
- Məlumatın bütövlüyü (Integrity): Məlumatın dəyişdirilmədiyini və orijinal olduğunu təmin etmək.
- İdentifikasiya və təhlükəsizlik (Authentication): Göndəricinin və alıcının kimliklərini təsdiq etmək və məlumatın mənbəyini müəyyənləşdirmək.
- Qeyri-İnkar Edilmə (Non-repudiation): Göndəricinin göndərilən məlumatı inkar etməsinin qarşısını almaq.

Metodlar

RSA şifrələmə texnikası, çox böyük tam ədədləri vuruqlara ayırmağın alqoritmik mürəkkəbliyindən istifadə edərək təhlükəsizlik təmin edir. Bu proses üçün iki fərqli böyük sadə ədəd seçilir. Gəlin RSA alqoritminin açar yaratma əməliyyatlarına bir nəzər salaq:

1. İlk növbədə, N ilə işarə ediləcək çox böyük tam ədədin yaradılması üçün iki fərqli və böyük sadə ədəd, p və q, seçilir.
2. Bu iki sadə ədədin hasilini tapırıq, çünki sadə vuruqlara ayırmaq daha mürəkkəbdir. Bu zaman N belə hesablanır:
$$N = p * q$$
3. N ədədinin totient dəyəri hesablanır.Totient, yəni $\varphi(N)$, bir tam ədədin o ədəddən kiçik və o ədəd ilə aralarında sadə olan ədədlərin sayını göstərən funksiyadır. Totient funksiyası Eyler tərəfindən müəyyən edilmiş və adətən Yunan hərfi φ ilə işarələnir:
$$\varphi(N) = (p - 1) * (q - 1)$$
4. 1 ilə $\varphi(N)$ arasında olan və $\varphi(N)$ ilə aralarında sadə olan bir tam ədəd seçilir və e olaraq adlandırılır. Bu, aşağıdakı şərtləri ödəmiş olmalıdır:
   $1 < e < \varphi(N)$
   ƏBOB(e, $\varphi(N)$) = 1
   Burada e-nin kiçik seçilməsi (məsələn, 5 kimi) əməliyyat performansını artırsa da, bəzən təhlükəsizliyi azalda bilər.
5. Məxfi (private) açar üçün istifadə ediləcək d ədədi tapılır. Bu, e-nin $\varphi(N)$-də tərsini tapmaqla həyata keçirilir. Genişlədilmiş Evklid alqoritmi bu əməliyyat üçün istifadə edilir:
   $d * e \equiv 1 \ (mod\ \varphi(N))$

Bu dəyişənlər yaradıldıqdan sonra, (N,e) cütü açıq açarı, (N,d) cütü isə məxfi açarı əmələ gətirir. Burada p, q və $\varphi(N)$ ədədləri məxfi qalmalıdır.

Şifrələmə prosesi – RSA ilə şifrələmə prosesində, göndəriləcək mətn alıcının açıq açarı (N, e) ilə şifrələnir ki, bu mesajı yalnız alıcı aça bilsin. Bunun üçün mesajın rəqəmsal qarşılığının e-ci qüvvəti mod N-də alınır:

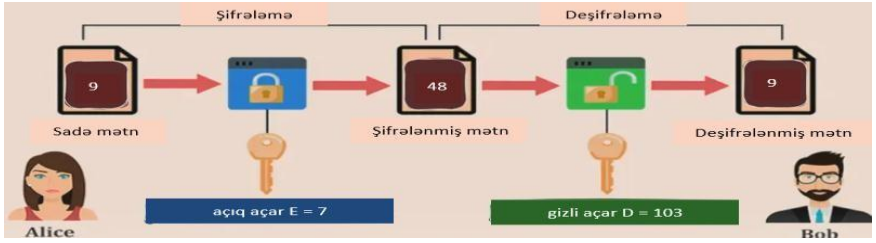
$$c = m^e \ (mod\ N)$$

Deşifrələmə prosesi – Açıq açarla şifrələnmiş bir mesaj yalnız o açıq açarın cütü olan məxfi açar (N, d) ilə deşifrə edilə bilər. Şifrələnmiş mətni açmaq üçün c-nin d-ci qüvvəti alınır və mod N-də qarşılığı tapılır:

$$m = c^d \ (mod\ N)$$

Bu şəkildə, şifrələnmiş məlumatı yalnız məxfi açara sahib olan alıcı oxuya bilər.

Bir nümunəyə nəzər yetirək:



Şəkil 1. RSA alqoritminin işləmə prinsipi

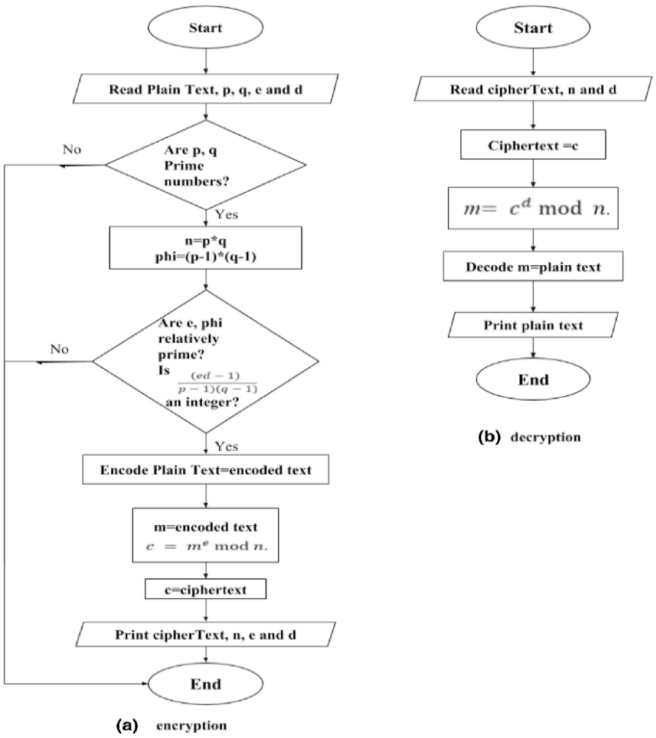
Alice, RSA açarlarını yaratmaq üçün iki sadə ədəd seçir: p = 11 və q = 13. Bu zaman N = p * q = 143 olur. Totient isə $\varphi(N) = (p-1) * (q-1)$ = 120 olaraq hesablanır. O, RSA açıq açarı üçün 7 ədədini seçir və genişlədilmiş Evklid alqoritmi vasitəsilə RSA məxfi açarını hesablayır ki, bu da 103 olur. Bob, Alice-ə şifrələnmiş mesaj göndərmək istəyir və onun RSA açıq açarını (n,e) əldə edir, bu misalda (143,7) olur. Bob-un açıq mətn mesajı sadəcə 9 ədədidir və bu, aşağıdakı kimi şifrələnir:

$$M^e \ mod \ n = \ 9^7 \ mod \ 143 = 48 = C$$

Alice, Bob-un mesajını aldıqda, RSA məxfi açarını (d,n) istifadə edərək onu deşifrə edir:

$$C^d \ mod \ n = \ 48^{103} \ mod \ 143 = 9 = M$$

Alice, mesajı Bob-a rəqəmsal olaraq imzalamaq üçün, əvvəlcə mesajın heş dəyərini yaratmalı və bu heş dəyərini RSA məxfi açarı ilə şifrələməlidir, daha sonra bu şifrələnmiş heş dəyərini mesaja əlavə etməlidir. Bob, heş dəyərini onun açıq açarı ilə deşifrə edərək mesajın Alice tərəfindən göndərildiyini və dəyişdirilmədiyini yoxlaya bilər. Əgər bu dəyər ilkin mesajın heş dəyəri ilə uyğun gələrsə, bu, mesajın Alice tərəfindən göndərildiyini və tam olaraq onun yazdığı kimi olduğunu təsdiq edər - autentifikasiya və təkzib edilə bilməzlik təmin edilir - və mesajın dəyişdirilmədiyi sübut olunur.



Şəkil 2. RSA alqoritminin blok sxeminin təsviri

Nəticə

RSA alqoritmi, kriptoqrafiya sahəsində ən mühüm və effektiv olan alqoritmlərdən biridir. Onun şəffaf və təhlükəsiz məlumat köçürməsini təmin etməkdəki mövqeyi, müasir dünyada mühüm bir yer işğal edir. Bu alqoritmin tətbiq sahələri çox genişdir. İnternet kommunikasiyasından məlumat qorunmasına, bank işlərindən məktəb sistemlərinə qədər bir çox sahədə RSA-nın əhəmiyyəti var.

Əsas fəaliyyət sahələri olan açar generasiyası, şifrələmə və deşifrə prosesləri, məlumatların təhlükəsizliyini təmin etmək üçün ən əsas amillərdən biridir. Açarların qorunması və effektiv istifadəsi, məlumatın əhəmiyyətini və dəyərini qoruyur. Həmçinin, RSA alqoritmi, açıq açarlı kriptoqrafiyanın ən məşhur nümunələrindən biri olduğu üçün, yeni tədqiqat və inkişaf sahələrinin də mərkəzi rolunu

oynayır. Lakin, dinamik kriptoqrafiya sahəsində, RSA alqoritmi də daim yenilənməyə və gücləndirməyə ehtiyac duyur. Bu, gələcəkdə məlumat təhlükəsizliyinin daha da təmin edilməsi üçün yeni inkişafların və təhlükəsizlik standartlarının qarşısının alınması ilə əlaqəlidir. Bu cür yeniliklər, RSA alqoritminin müasir məlumat təhlükəsizliyinə daha da çox uyğunlaşmasını təmin edəcək və onun tətbiq sahələrini daha da genişləndirəcəkdir.

Ədəbiyyat

[1] Boneh, D. (2018). *Introduction to Cryptography*. Course notes. Retrieved from https://crypto.stanford.edu/~dabo/cryptobook/

[2] Chen, L., & Li, J. (2013). A note on the RSA key generation algorithm. *Journal of Applied Mathematics*, 2013, Article ID 758105.

[3] Ding, J., & Wang, X. (2019). RSA algorithm in cloud computing. *Journal of Cloud Computing*, 8(1), 20.

[4] Gao, S., & Shen, S. (2017). Improving the efficiency of RSA key generation. *IEEE Transactions on Information Forensics and Security*, 12(5), 1137-1147.

[5] Huang, J., & Zhang, Y. (2018). Analysis of RSA cryptosystem. *International Journal of Network Security*, 20(5), 856-861.

[6] Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography*. CRC Press.

[7] Khodari, M., & Salah, K. (2015). Enhancing RSA algorithm for public key encryption. *Procedia Computer Science*, 56, 117-125.

[8] Kim, H., & Lee, J. (2017). A new approach to RSA key management in IoT environments. *Sensors*, 17(11), 2485.

[9] Knežević, M., & Akleylek, S. (2016). Secure RSA implementation against side-channel attacks. *Journal of Cryptographic Engineering*, 6(4), 251-261.

[10] Lee, B., & Chang, H. (2019). A study on RSA algorithm for secure communication. *Information*, 10(1), 19.

[11] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2016). *Handbook of Applied Cryptography*. CRC Press.

[12] Paterson, K. G., & Schuldt, J. (2013). Efficient RSA key generation for embedded devices. *IEEE Transactions on Information Forensics and Security*, 8(5), 773-782.

[13] Smart, N. P. (2018). *Cryptography Made Simple*. Springer.

[14] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

[15] Yan, Q., & Yang, H. (2014). An improved RSA encryption algorithm based on FPGA. *International Journal of Security and Its Applications*, 8(1), 237-244.

INFORMASİYA TƏHLÜKƏSİZLİYİ SİYASƏTİNƏ UYĞUNSUZLUQ: KAPİTULYASİYA NƏZƏRİYYƏSİ VƏ İSTİFADƏÇİ DAVRANIŞLARI

Məmmədzadə Nəcəf
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə

Məqalədə bu məsələlər ətraflı şəkildə müzakirə olunur. Kapitulyasiya nəzəriyyəsinin anlamı və informasiya təhlükəsizliyi siyasətinə qarşı təsiri ayrıntılı şəkildə izah edilir. İstifadəçilərin bu nəzəriyyəyə meyilliyyəti və onların informasiya təhlükəsizliyi ilə bağlı davranışları təhlükələrə səbəb ola bilən məsələlər kimi müzakirə olunur. İstifadəçi davranışlarının informasiya təhlükəsizliyinə təsiri və riskli davranış nümunələri də qeyd olunur. Nəticədə, informasiya