important to capture and was implemented throughout documentation. During the trials of these interactions, it became apparent to all teams that the coming together of these multiple disciplines was beneficial to the overall understanding of issues and effective resolution techniques. The knowledge that projects developed in other faculties had the potential to resolve similar issues and interest in the attendance tracking automation was widespread. A service-oriented architecture style was employed, and proof of concepts demonstrated a web service to book study spaces and interface developments to the tracking system using RFID. With the technology's success in the academic environment and potential to be applied across the university, foresights to future developments and collaboration between faculties were included in development and deployment plans.

References

[1] A. Jarrett and K. K. R. Choo, "The impact of automation and artificial intelligence on digital forensics," Wiley Interdisciplinary Reviews: Forensic Science, vol. 2021. Wiley Online Library. [HTML]

[2] N. S. Ali, A. H. Alhilali, H. D. Rjeib, "Automated attendance management systems: systematic literature review," International ..., 2022, inderscienceonline.com. researchgate.net

[3] P. Chakraborty, C.S. Muzammel, M. Khatun, et al., "Automatic student attendance system using face recognition," International Journal of ..., 2020. academia.edu

[4] U. Khamdamov, A. Abdullayev, J. Elov, "Conceptual model of the education management information system for higher education institutions," International Journal of ..., 2020. [Online]. Available: researchgate.net. researchgate.net

[5] S. Elaskari, M. Imran, A. Elaskri, and A. Almasoudi, "Using barcode to track student attendance and assets in higher education institutions," Procedia Computer Science, 2021. sciencedirect.com

[6] A. B. Rensfeldt and L. Rahm, "Automating teacher work? A history of the politics of automation and artificial intelligence in education," Postdigital Science and Education, 2023. springer.com

[7] AA Raj, M Shoheb, K Arvind, "Face recognition based smart attendance system," in Proc. ... conference on intelligent ..., 2020. [HTML]

[8] D. Ozdemır and M. E. Ugur, "Model proposal on the determination of student attendance in distance education with face recognition technology," Turkish Online Journal of Distance Education, 2021. dergipark.org.tr

[9] A. Nuhi, A. Memeti, F. Imeri, B. Cico, "Smart attendance system using qr code," in 2020 9th Mediterranean Conference on Embedded Computing (MECO), 2020, pp. 1-4. [HTML]

[10] K. Alhanaee, M. Alhammadi, N. Almenhali, et al., "Face recognition smart attendance system using deep transfer learning," in Procedia Computer Science, vol. 179, Elsevier, 2021. sciencedirect.com

[11] Qureshi, M. (2020). The proposed implementation of RFID based attendance system. International Journal of Software Engineering & Applications (IJSEA), 11(3). academia.edu

RSA ALQORİTMİNİN RİYAZİ VƏ PROQRAM TƏMİNATININ İŞLƏNMƏSİ

Əsgərov Taleh, Adil Şəfizadə
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə

Kriptoqrafik alqoritmlər, məlumatları müstəqil və təhlükəsiz bir şəkildə ötürmək və saxlamaq üçün istifadə olunan texnologiyalardır. Bu texnologiyalardan biri də RSA alqoritmidir. Asimmetrik şifrələmə növü olan RSA alqoritmi mesajların şifrələnməsi və deşifrə edilməsi üçün geniş istifadə olunur. RSA alqoritminin necə işlədiyini başa düşmək üçün ilk növbədə açıq və gizli açarlar anlayışını başa düşməliyik. RSA alqoritmində hər bir istifadəçinin bir cüt açarı var: açıq açar və şəxsi açar. Açıq açar istifadəçiyə mesaj göndərmək istəyən hər kəs üçün əlçatan olur və ondan mesajı şifrələmək üçün istifadə olunur. Şəxsi

açar məxfi saxlanılır və mesajın şifrəsini açmaq üçün istifadə olunur. RSA alqoritminin təhlükəsizliyi, böyük bir kompozit ədədi onun əsas bölənlərinə ayırmağın hesablama baxımından qeyri-mümkünlüyüdür. Başqa sözlə, iki böyük sadə ədədin hasili olan bir ədədi nəzərə alsaq, bu sadə ədədlərin nə olduğunu anlamaq çox çətindir. Bu, RSA alqoritminin əsasını təşkil edir. Həmçinin RSA məlumatların müəyyən bir şəxs tərəfindən göndərildiyini doğrulamaq üçün də istifadə olunur. Bu zaman rəqəmsal imzalardan istifadə olunur.

Açar sözlər: kriptoqrafiya, şifrələmə, deşifrələmə, açarlar, RSA, təhlükəsizlik, sadə ədədlər.

Giriş

1977 -ci ildə, Ron Rivest, Adi Shamir və Leonard Adleman rəqəmsal şifrləmə alqoritmini təqdim etdilər ki, bu əsasən daha az təhlükəsiz Milli Standartlar Bürosunun (NBS) alqoritmini əvəz etmək üçün idi. RSA əsasən açıq-açarlı şifrləmə sistemi və digər rəqəmsal imzaları həyata keçirir. RSA, əvvəlcədən bəhs edilən, lakin əslində inkişaf etdirilməmiş olan Diffie və Hellman'ın dərc olunan əsərlərindən ilham alınaraq hazırlanmışdır. [1]

Elektron poçt dövrünün tezliklə başlayacağı gözlənilən vaxtda təqdim edilən RSA, iki əsas fikri həyata keçirirdi:

1. **Açıq açarla şifrələmə.** Hər kəsə açıq olan şifrələmə metodudur. Bu metodda, iki ana açıq və gizli açar istifadə olunur. Açıq açar hər kəs tərəfindən bilinir və məlumatların şifrələnməsi və ya şifrənin açılması üçün istifadə olunur. Gizli açar isə yalnız məlumatın sahibi tərəfindən bilinir və məlumatları açmaq üçün istifadə olunur. Bu metod əsasən təhlükəsizliyi artırmaq və məlumatların mübadiləsini təmin etmək üçün istifadə olunur. Bu fikir, təyin edilmiş mesajı göndərmədən əvvəl alıcıya açarları başqa bir təhlükəsiz kanal vasitəsilə çatdırmaq üçün bir "kuryer"ə ehtiyacı aradan qaldırır. RSA'da şifrələmə açarları açıq, deşifrə etmə açarları isə gizlidir, buna görə də yalnız düzgün deşifrə etmə açarına malik olan biri şifrəli mesajı açа bilər. Hər kəs öz şifrələmə və deşifrə etmə açarlarına malikdir. Açıq şifrələmə açarından deşifrə etmə açarının asanlıqla çıxarılmaması üçün açıq açarlar uyğun şəkildə hazırlanmalıdır.
2. **Rəqəmsal imza.** Rəqəmsal imzalama, məlumatların doğruluğunu, bütövlüyünü və autentikliyini təmin etmək üçün istifadə olunan bir texnologiyadır. Bu metodda, məlumat özünə məxsus bir rəqəmsal imza ilə imzalanır. İmza, məlumatın göndərən tərəfindən yaradılır və açıq açar istifadə edilərək yoxlanılır. Bu, məlumatın dəyişdirilməməsinə və göndərənin kimliyinə əmin olmağa kömək edir. Beləliklə, imzalar saxta edilə bilməz. Həmçinin, imza atan sonra imzaladığını inkar edə bilməz.

Bu, yalnız elektron poçtlar üçün deyil, digər elektron əməliyyatlar və köçürmələr üçün də faydalıdır, məsələn, vəsait köçürmələri kimi. RSA alqoritminin təhlükəsizliyi sınanmışdır, hələlik heç bir cəhd onu sındırmaq üçün uğurlu nəticələnməmişdir. Bu, böyük məsələlərin faktorlanmasının çətinliyi ilə bağlıdır. $n = pq$, burada p və q böyük sadə ədədlərdir. [2]

İşin məqsədi

RSA -nın əsas məqsədi, məlumatların güvənli və qorunmuş bir şəkildə ötürülməsini və mübadiləsini təmin etməkdir. Bu, internet əlaqələrində, VPN-lərdə elektron ödəniş sistemlərində, məktəblər və şirkətlərdə məlumatların şifrələnməsində, electron poçt və şəxsi məlumatların müdafiəsində istifadə olunur. RSA alqoritmi üç əsas prosesdən ibarətdir: Açıq açar yaradılması, məlumatların şifrələnməsi və dəşifrə olunması.

1. Açıq açar yaradılması: İki özəl asal ədəd seçilir, buna "p" və "q" deyilir. Bu ədədlərdən biri digərindən fərqli ola bilməlidir. Sonra $n = p \times q$ hesablanır. Bundan sonra, $\varphi(n) = (p-1) \times (q-1)$ hesablanır. Ən sonda, ən böyük ortaq bölünənə əsaslanan bir "e" ədədi seçilir ki, 1-dən və $\varphi(n)$ -dən böyük olsun və ən böyük ortaq bölünəni olmasın. Bu "e" açıq açar olaraq tanımlanır.
2. Məlumatların şifrələnməsi: Məlumat "m" şifrələnmək istədikdə, əvvəlcə məlumat "c" olaraq şifrələnir. $c = m^e \ mod \ n$ hesablanır.
3. Deşifrə olunması: Şifrələnmiş məlumat "c" dəşifrə olunarkən, əvvəlcə dəşifrə açar "d" hesablanır. $d = e^{(-1)} \ mod \ \varphi(n)$ formula ilə tapılır. Sonra, $m = c^d \ mod \ n$ hesablanır və məlumat dəşifrə edilir.

İstifadə edilən metodlar

1) Açıq açarlı kriptosistemlər. Hər bir istifadəçinin öz şifrələmə və deşifrələmə prosedurları var, E və D, birincisi açıq faylda, ikincisi isə gizli saxlanılır. Bu prosedurlar RSA istiqamətində düzəldilmiş açarlarla əlaqəlidir, ki, məhz, iki xüsusi rəqəmdən ibarət dəstlərdir. Biz təbii ki, əvvəlcədən M ilə təsvir olunan mesajla başlayırıq, hansı ki, bu şifrələnəcək. Bir açıq açarlı şifrələmə sistemi üçün xüsusi və əsas dörd prosedur var:

a) Şifrələnmiş bir mesajı deşifr etmək sizə xüsusi olaraq orijinal mesajı verir.

$$D(E(M)) = M$$

b) Prosedurları tərsinə çevirəndə hələ də M-i əldə edirik:

$$E(D(M)) = M$$

c). E və D hesablaması asandı

d). E-nin ictimailiği, D-nin sirrini təhluksüz etmir, yəni E-dən D-ni asanlıqla anlaya bilməzsiniz. Verilmiş E ilə, D-ni hesablamaq üçün sərfəli bir yol verilmir. Əgər $C = E(M)$ şifrəli mətndirsə, D-ni tapmaq üçün $E(M) = C$ əməliyyatını yerinə yetirmək məsələsi aşağı dərəcədə mümkündür. Çünki sınaq olunacaq mesajların sayı praktiki olaraq çox böyük olar.

(a), (c) və (d) şərtlərini ödəyən E, "tələ qapısı birtərəfli funksiyası" adlanır və eyni zamanda bir "tələ qapısı birtərəfli permutasiyası"dır. Bir məlumat yığınına "qapan" kimi baxılmasının səbəbi, o məlumatlara əsasən, tərs prosesi - D-ni asan hesablamaq üçün əlavə "qapan-çıxarma" məlumatlarının mövcud olması, əks halda isə hesablamanın çətin olmasıdır. Bu, hesablamanın bir istiqamətdə asan, digər istiqamətdə çətin olduğu üçün birtərəfli prosesdir. Bu, hər şifrələnmiş mətnin bir potensial mesaj olduğu və hər mesajın digər mətnin şifrələnməsi olduğu (b) şərtini ödədiyi üçün bir permutasiyadır. Həqiqətdə (b) ifadəsi sadəcə "imza" vermək üçün lazımdır. Qeyd olunan açarlar üzrə iki istifadəçi götürsək A (Aslan) və B (Babək), onların açarları E_A,E_B və D_A, D_B olar. [3]

2) Gizlilik. Şifrələmə, indi gizli bir şəkildə mesajın çatdırılmasını təmin etməyin yaygın bir yolu olaraq istifadə olunur və bu, hər hansı bir təxribatçının şifrələnmiş mətni keçə bilməməsini təmin edir, əsasən ağ səs kimi. Lakin, özəllikə (d) olmadan, şifrələmə prosesi hələ də açıq açarlı deyil, məsələn, NBS standartı kimi. Bu, açarların digər təhlükəsiz bir "kuryer" vasitəsilə gizli şəkildə çatdırılması tələb edir, ki, NBS-ni, məsələn, yavaş, effektivsiz və beləliklə də ehtimal olaraq bahalı edəcəkdir. Beləliklə, RSA bu problemə böyük bir cavab olaraq göstərilir. NBS standartı yalnız RSA-dan sürətli bir alqoritm olduğu halda faydalı olardı, ki, RSA yalnız açarların təhlükəsiz bir şəkildə ötürülməsi üçün istifadə edilərdi. Beləliklə, RSA-nın tamamilə müstəqil və etibarlı olmasını təmin etmək üçün D-nin effektiv bir hesablama metodunun tapılması lazımdır ((c)-nin tələbi). [4]

İndi, Babək Aslana gizli bir mesaj göndərmək istəyir. O E_A açarını açıq fayldan alacaq, M-i şifrələyəcək və $C = E_A(M)$ əldə edəcək. Daha sonra, Aslan öz D_A açarı ilə onu deşifr edəcək ki, bu, yalnız onun edə biləcəyi bir işdir, (d) özəlliyindən dolayı. O da E_B ilə cavab verə bilər. Beləliklə, bu kriptosistemə hər iki istifadəçinin, öz şifrələmə məlumatlarını açıq fayla yerləşdirərək qatılmağı razılığa gətirmək lazımdır. Əvvəlcədən əlaqələşmə, gizli və ya açıq, lazım deyil. Həmçinin, (d) özəlliyindən dolayı, gözləyən tərəf E-ni eşidərək D-ni çıxara bilməz.

3) İmzalar. Mesajın məlum göndəricidən gəldiyinə əminlik üçün mesajla birlikdə bir rəqəmsal imza lazımdır. Rəqəmsal imza rəqəmsal mesajların və ya sənədlərin həqiqiliyini yoxlamaq üçün riyazi sxemdir. Mesajda etibarlı rəqəmsal imza alıcıya mesajın alıcıya məlum olan göndəricidən gəldiyinə əminlik verir. Rəqəmsal imzalar tez-tez elektron imzaların həyata keçirilməsi üçün istifadə olunur , bunlara imza niyyətini daşıyan hər hansı elektron məlumat daxildir, lakin bütün elektron imzalar rəqəmsal imzadan istifadə etmir. [5]

4). Tətbiqlər, proqnozlar, hardware tətbiqi.

Tətbiqlər: Təhlükəsizliyin məxfiliyi: RSA, məlumatın şifrələnməsi və deşifrələnməsi üçün istifadə olunur. Bu, internet üzərində sürətlə paylaşılan məlumatın təhlükəsizliyini təmin etmək üçün ən çox istifadə olunan metodlardan biridir. HTTPS protokolu kimi təhlükəsiz veb saytları, SSH kimi təhlükəsiz

uzak keçidlər, və PGP kimi məktublaşma protokolları RSA ilə məlumatın şifrələnməsi üçün istifadə edir. RSA alqoritmi tətbiq edildiyi sahələrdə geniş mövqe tutur. İşinizi ən çox nüfuzlu təhlükəsizlik məqsədləri üçün istifadə etməklə birlikdə, RSA da elektron məktubları, bank xidmətləri, elektron ticarət və daha bir çox sahədə istifadə olunur. RSA, məlumatın təhlükəsiz şəkildə şifrələnməsini və məlumatların əlavə təhlükəsizlik prosedurları əldə edilməsini təmin edir. Bu alqoritmin pratik tətbiqi, güvənli və şəffaflıq tələblərinə cavab verən çox sayda müxtəlif şəxsi və iş tətbiqatlarına nəzarət etmək üçün əlverişlidir.

Rəqəmsal imza**:** RSA, məlumatın doğruluğunu təsdiq etmək üçün də istifadə olunur. Rəqəmsal imzalar, bir mənbədən gəldiyini və dəyişdirilmədiyini təsdiq edən elektronik imzalar kimi tətbiqlərdə istifadə olunur.

Proqnozlar: RSA, müasir kriptoqrafiyanın ən əhəmiyyətli algoritmalarından biri olaraq qalır və ən müasir təhlükəsizlik standartlarında istifadə olunur. Lakin, daha güclü kriptoqrafiya tələbləri və nümunələrə görə, daha uzun açarlar tələb edən alternativ algoritmaların inkişafı proqnoz edilir.

Aparat təminatının qurulması: RSA algoritmi, həm yazılım, həm də hardware implementasiyalarında tətbiq oluna bilər. Xüsusi tələblərə görə, RSA algoritminin performansını artırmaq üçün xüsusi kriptoqrafiya işləyiciləri (cryptographic accelerators) və ya spesifik hardware cihazları inkişaf etdirilir. Bu, RSA əməliyyatlarını daha sürətli həyata keçirərək tətbiqatlarda performansı artırmağa kömək edir. [6]

5) RSA-nın riyazi hesablanması. RSA-da $e \times d = 1\ mod\ (p-1) \times (q-1)$ ödəyən iki böyük p və q əsas dəyərimiz var, modul N = pq, şifrələmə göstəricisi e, şifrə açma eksponenti isə d-dir. Açıq açar cütdür (N, e), gizli açar isə d-dir.

M mesajını şifrələmək üçün, $C = M^e\ mod\ N$ hesablayın.

Biz $M = C^d\ mod\ N$ -ni göstərmək istəyirik, yəni C şifrəli mətnini d gücünə yüksəltməklə və nəticə modulunu N azaltmaqla şifrəni açа bilərik. m və n iki müsbət tam ədədlərinin 1-dən başqa ortaq bölənləri yoxdursa, *onlar qarşılıqlı sadə ədədlər* adlanır. Məsələn, həm 10, həm də 9 mürəkkəb ədədlər olsa da, onlar qarşılıqlı sadədirlər, çünki onların heç bir ortaq böləni (1-dən başqa) yoxdur.

Müsbət n tam ədədi üçün φ(n) n ilə qarşılıqlı sadə olan n-dən kiçik tam ədədlərin sayı kimi təyin edilir. Məsələn, $\varphi\ (12) = 4$, çünki yalnız 11, 7, 5 və 1 12-dən kiçikdir və 12-ilə qarşılıqlı sadədir. Bundan başqa, $\varphi\ (7) = 6$. Yəni, istənilən sadə p ədədi üçün bizdə $\varphi(p) = p - 1$.

Tutaq ki, n-nin əsas faktorlara ayrılması, $n = p_1^{k1} p_2^{k2} \dots p_r^{kr}$ ilə verilir, onda,

$\varphi(n) = n\,(1 - 1/p_1)(1 - 1/p_2)\dots(1 - 1/p_r)$ olduğunu göstərmək olar. Qeyd edək ki, RSA modulu N = pq üçün bu nəticə $\varphi(N) = (p-1)(q-1)$ deməkdir.

Bizə lazım olan son riyazi nəticə Fermanın Kiçik Teoremidir. Bu teorem adətən belə ifadə edilir:

Fermanın kiçik teoremi: Əgər p sadədirsə və p, x-i bölmürsə, $x^{p-1} = 1\ mod\ p$.

Bununla belə, Fermanın Kiçik Teoreminin ümumiləşdirilməsi (bəzən Eyler teoremi kimi də tanınır) RSA üçün daha birbaşa tətbiq olunur. Bu teorem aşağıdakı kimidir. Eyler teoremi: Əgər x, n ilə qarşılıqlı sadədirsə, $x^{\varphi(n)} = 1\ mod\ n$. İndi RSA deşifrəsinə qayıdaq. Göstərmək istəyirik ki,

$$M = C^d = (M^e)^d = M^{ed}\ mod\ N.$$

Xatırladaq ki, $ed = 1\ mod\ (p-1)(q-1)$. Həmçinin, N = pq olduğundan, yuxarıda qeyd edildiyi kimi, bizdə

$$\varphi(N) = (p-1)\,(q-1)$$ var.

Bundan belə nəticə çıxır ki, $ed = 1\ mod\ \varphi(N)$.

Onda "mod"un tərifinə görə elə bir k var ki, $ed - 1 = k\varphi(N)$. Bizdə,

$$M^{ed} = M^{(ed-1)+1} = M\,M^{ed-1} = M\,M^{k\varphi(N)}\ mod\ N$$ var.

Nəhayət, nəticəni vermək üçün Fermanın Kiçik Teoremi (Eyler teoremi şəklində) tətbiq oluna bilər.

$$M^{ed} = M\,(M^k)^{\varphi(N)} = M\ mod\ N = M.$$ [7]

6) RSA nə dərəcədə təhlükəsizdir? RSA algoritmi həqiqətən də ən güclü alqoritmlərdən biri olaraq tanınır, lakin hər şeyə dayanıqlı olmaq olarmı? Əlbəttə ki, zamanın sınağına dayanmaq mümkün deyil.

Əslində, həç bir şifrələmə texniki həqiqətən də bir riyaziyyat təcrübəçisinin hücumundan müdafiə oluna bilməz. Bizim ehtimal yanaşmasını da nəzərə almağımız lazımdır, bu o deməkdir ki, həmişə birinin "bir milyon açardan birini əldə etmə" ehtimalı mövcuddur. [8]

7) İmzalanmış bir mesajın şifrələnməsində "yenidən bloklama"dan imtina etmək. "Reblocking" ifadəsi imzalanmış bir mesajı daha kiçik bloklara bölərək işləmək mənasını verir, çünki imza n dəyəri şifrələmə n dəyərindən böyük ola bilər (hər ikisi də fərqli istifadəçilərin müxtəlif açarlarından gəldiyi üçün fərqlidir). RSA'nın müəllifləri isə bir mesajın reblocking-dən imtina etmək üçün bir yol təqdim etmişlər: Açıq açarlı kriptosistem üçün eşik dəyəri seçək: h (məsələn, $h = 10^{202} - 33$). Hər istifadəçi iki ictimai (e, n) cütlüyünü saxlayır. Bunlardan bir cütü şifrələmək üçün, digəri isə imza doğrulaması üçündür. Ənənəvi olaraq, hər bir imzanın n dəyəri h-dan kiçik, hər bir şifrələmənin n dəyəri isə h-dan böyükdür. Beləliklə, mesaj bloklama yalnız göndərənin imza n dəyərinə bağlı olacaq. Beləliklə, mesaj bloklama yalnız göndərənin imza n dəyərinə bağlı olacaq. [9]

8). RSA -ya yönəlmiş təhlükələr.

- Faktorizasiya hücumları: RSA-nın təhlükəsizliyi, böyük mədəniyyətə sahib rəqəmlərin faktorizasiya edilməsinin çətinliyindən asılıdır. Yenilikçi faktorizasiya alqoritmləri və güclü kompüterlər təhlükəsizliyi pozur və böyük rəqəmləri daha tez faktorizasiya edə bilər.
- Zamanlama hücumları: Zamanlama hücumları, məlumatın işləmə vaxtına görə məlumat toplamaq və təhlükəsizliyi nümayiş etmək üçün istifadə edilir. RSA-da istifadə olunan əməliyyatlar zamanla dəyişikliklərə məruz olduğu üçün bu cür hücumlar təhlükəlidir.
- Açarlar daxilində sızıntılar: RSA-da istifadə olunan açarlar həmin açarların daxilində sızıntılar olduğu və bu sızıntılar vasitəsilə qarşı tərəf RSA-nın məlumatlarını deşifrə etmək istifadə edilir.
- Quantum Computing**:** Quantum kompüterlərin inkişafı RSA-da müxtəlif hücumlar üçün böyük bir təhlükə təşkil edir. Bu kompüterlər, RSA-nın təhlükəsizliyini pozmaq üçün ən effektiv faktorizasiya alqoritmlərini tətbiq edə bilərlər [10].

Vaxt keçdikcə daha effektiv faktorizasiya alqoritmləri yaradıldıqca və kompüterlər sürətlənəndikcə, n-nin ortalama ölçüsü artmalıdır. Bu, RSA açarları üzərində gələcəkdə mövcud təhlükələrin azalmasına kömək edir. 1978-ci ildə, RSA-nın müəllifləri üçün n dəyərləri üçün 200 rəqəm uzunluğu təklif edildi. "2008-ci ildə, ümumi məqsədli faktorizasiya alqoritmi ilə faktorizasiya olunmuş ən böyük (bilinən) rəqəm [200 rəqəm (663 bit) uzunluğundaydı]". Hazırda, RSA açarları tipik olaraq 1024 və 2048 bit uzunluğunda olur, ki, bu da müəlliflərə görə yaxın gələcəkdə kırılabilir. Hələlik, 4096 bitlik açarların yaxın bir vaxtda kırılmasına heç kim şahid olmayıb. Hazırda, bir PC-də bir neçə saat ərzində faktorizasiya edilə bilən n, 300 bitdən uzun olmamalıdır, buna görə də açarlar tipik olaraq bugünkü vaxtlarda 4-7 dəfə daha uzundur [11] Simmetrik kriptosistemlərə nisbətən RSA daha yavaşdır. RSA əsasən daha az təhlükəli, amma daha sürətli bir alqoritmin açarlarını təhlükəsiz şəkildə ötürmək üçün yaygın şəkildə istifadə olunur. Əslində, RSA-nın təhlükəsizliyini potensial olaraq ziyan verə biləcək bir neçə məsələ mövcuddur. Məsələn, zamanlama hücumları və açarların paylanması ilə bağlı problemlər kimi, bunların da həlləri mövcuddur.

RSA-nı tətbiq edən hər hansı bir cihazın, müxtəlif hücumlara və casusluq cəhətlərinə qarşı müdafiə üçün daha geniş hardware və software -yə sahib olması tələb olunur. RSA üçün ən böyük təhlükə Riemann hipotezinin həll edilməsi olardı. Hələlik belə bir həllin var və ya yox olması sübut edilməyib. Riemann hipotezi ilə bağlı işlər indi nisbətən dayanmış vəziyyətdədir. Lakin, əgər bir həll tapılsa, sadə ədədləri tapmaq çox asanlaşar və RSA zəiflənərək iflasa uğrayar. Qeyd edək ki, riyaziyyatçılar daha çox nömrələr teoremi və kriptoanaliz sahələrində çalışdıqca, RSA-dan daha kompleks alqoritmlər tərtib edəcəklər. RSA alqoritminə aid pythonda icra edilmiş, rəqəmlərin şifrələnmə və deşifrələnməsinə aid proqram nümunəsi aşağıdakı fraqmentdə verilmişdir.

Şəkil. Proqram təminatından fraqment

Nəticə.
RSA zamanın sınağından keçmiş güclü bir şifrələmə alqoritmidir. RSA, təhlükəsiz kommunikasiyalar və "rəqəmsal imza" imkanı verən açıq açarlı kriptosistem təqdim edir, və onun təhlükəsizliyi böyük rəqəmlərin faktorizasiya çətinliyinə dayanır. Müəlliflər, hər kəsi onların kodunu faktorizasiya texnikaları ilə və ya başqa yollarla sınamağa çağırırdılar, ancaq hələlik heç kimsə uğur əldə etməyib. Bu, əsasən RSA-nın təsdiq edilməsinə səbəb olmuş və bu cür müdafiəsiz girişlərə qarşı vaxtın sınağına qədər təhlükəsizliyini təmin edəcəkdir.

Ədəbiyyat.

[1] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography", CRC Press, 2014. – (səh 312)
[2] "Public-Key Cryptography: Theory and Practice" - Bodo Möller, Michael Brenner,Shai Halevi (2021) - (səh 185)
[3] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson, 2016. (səh 294)
[4] https://www.geeksforgeeks.org/rsa-algorithm-cryptography
[5] Dan Boneh, Victor Shoup, "A Graduate Course in Applied Cryptography", 2020. (səh 400)
[6] https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm
[7] https://www.techtarget.com/searchsecurity/definition/RSA
[8] https://www.javatpoint.com/rsa-encryption-algorithm
[9] https://link.springer.com/referenceworkentry/10.1007/0-387-30038-4_206
[10] https://www.educba.com/rsa-algorithm/
[11] https://www.securityweek.com/in-other-news-rsa-encryption-attack-meta-ai-privacy-shinyhunters-hacker-guilty-plea/

ÖYRƏTMƏ İDARƏETMƏ SİSTEMLƏRİ

Əsgərov Taleh
Bədəlova Nərgül
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə
Məqalə təhsil sahəsində öyrətmə idarəetmə sistemləri və ya LMS (Learning Management System) haqqında ümumi məlumat verir. Burada öyrətmə idarəetmə sistemlərinin tarixi, istifadələri, növləri tədqiq olunmuşdur. Bununla bərabər LMS-lərin alətləri, üstünlükləri və çətinlikləri, o cümlədən Azərbaycanda tətbiqi öz əksini tapmışdır. Öyrətmə idarəetmə sistemləri son dərəcə əhəmiyyətli alətlər və bir çox üstünlüklər təqdim etməklə öyrənmənin effektivliyini və tələbələrin motivasiyasını artırır. Sözügedən sistemlərin tətbiqi tələbələrin təhsil təcrübələrinin artırılması və akademik nəticələrinin yaxşılaşdırılmasına yönəldilmişdir. Bununla yanaşı, LMS-lərin qarşılaşdığı interfeys dizaynı, internet bağlantısı, texniki savad, texnoloji bilik və bacarıqlar, o cümlədən pedaqoji uyğunlaşma kimi bir sıra problemlər var və onları araşdırmaq lazımdır. Belə ki, qeyd olunan bu problemlər öyrətmə idarəetmə sistemlərinin səmərəli tətbiqinə mane olur.

Açar sözlər: Öyrətmə idarəetmə sistemləri, öyrətmə idarəetmə sistemlərinin alətləri, öyrətmə idarəetmə sistemlərinin növləri, üstünlüklər, çətinliklər, onlayn təhsil.

Giriş