tools for graph database management are steadily addressing these hurdles. In essence, graph databases serve as a vital tool for dissecting and processing complex data relationships. Their utilization can yield more efficient and precise outcomes across diverse fields.

References

[1] "Next Generation Databases" by Guy Harrison
[2] "InavoluGRAPH DB WITH NEO4J" by Satya Srikanth Inavolu
[3] "Graph Database Modeling With Neo4j" by Ajit Singh
[4] https://bigdataschool.ru/blog/graph-database-under-the-hood.html
[5] https://appmaster.io/ru/blog/arkhitektura-programmnogo-obespecheniia-grafovykh-baz-dannykh
[6] https://www.oracle.com/autonomous-database/what-is-graph-database/
[7] https://www.decube.io/post/graph-database-concept
[8] "Graph Databases" - Lan Robinson, Jim Webber & Emil Eifrem
[9] "Graph Databases For Beginners" - Bryce Merkl Sasaki, Joy Chao & Rachel Howard
[10] "Graph Databases" -Adrian Silvescu, Doina Caragea, Anna Atramentov
[11] https://ericvanier.com/next-generation-database-architectures-for-scale-and-performance/
[12] https://ericvanier.com/next-generation-data-management-trends-and-opportunities-in-2023/
[13] https://wiki.merionet.ru/articles/chto-takoe-grafovaya-baza-dannyh
[14] https://aws.amazon.com/ru/compare/the-difference-between-graph-and-relational-database/

DİFFİE-HELMAN ALQORİTMİ VƏ ONUN TƏTBİQİ

Fidan Paşayeva
"R.İ.S.K. Elmi İstehsalat Şirkəti" Qapalı Səhmdar Cəmiyyəti

Xülasə

Əsas məqsəd, məlumatın təhlilində, özünü qorumaq və mübahisəsiz məlumatı mübadilə etmək üçün təhlükəsiz bir platform yaratmaqdır. Ənənəvi kriptoqrafiyanın əsas problemlərindən biri, məlumatı açıq şəkildə göndərən və qəbul edən tərəflərin müxtəlifliklərı ilə əlaqədar olan təhlükələrdir. Diffie-Hellman alqoritmi, bu problemləri həll etmək üçün inkişaf etdirilmiş bir protokoldur. Sözügedən alqoritmi, açıq şifrələmə əsasında əsaslanır və iki tərəf arasında gizli açarları mübadilə etmək üçün istifadə olunur. Bu alqoritmin əsas fikri, bir məlumatın qorunmasında məlumatın özünü deyil, özü üçün gizli olan açarların bir müddət sonra dəyişməsi ilə əlaqəlidir. Bu, qarşı tərəf məlumatı şifrələmək və açmaq üçün birbirilərindən asılı olan açarları yaratmaq imkanı verir. Diffie-Hellman alqoritmi, məlumatın müəyyən edilməsinin asanlaşdırılması ilə əlaqədar olan ənənəvi kriptoqrafiya texnikalarından fərqlənir. Bu alqoritmin əsas qüsurları arasında həmin məlumatın qarşı tərəf tərəfindən mənimsənilməsinin qeyri-mümkünlüyü və ələ keçirilmə riski sayılmaqdadır. Əksinə, həmin haqqında söz açılan alqoritmi, təhlükəsiz şifrələməni təmin etmək və gizliliyi qorumaq üçün innovativ bir yanaşma təklif edir. Bu konfrans, Diffie-Hellman alqoritminin əsas prinsiplərini, işləmə mexanizmini və təhlükəsizliyini izah edəcək. Həmçinin, alqoritmin mövcud tətbiq sahələri və müasir məqamları da müzakirə olunacaq. Bu konfrans, kriptoqrafiya sahəsində yenilikləri axtarış və təşviq etməyə həsr edilmişdir. Məqaləmin mövzusu "Diffie-Hellman Alqoritmi və Onun Tətbiqi". Bu alqoritmin təsviri və əsas prinsipləri təqdim olunacaq. İlk olaraq, Diffie-Hellman alqoritminin məqsədi və əhəmiyyəti açıqlanacaq. Sonra, əsas

alqoritmin əsas prinsipləri izah ediləcək və əməli tətbiqatları üçün təklif olunan bəzi sahələr müzakirə olunacaq. Əsas prinsiplərə baxdıqda, iki əsas hissəni nümayiş etdirir: birincisi, ənənəvi şifrələmə sistemləri ilə müqayisədə, açıq açar mübadiləsində qəbul edilmiş bir istifadəçi tərəfindən istifadə edilən gizli açarın olmaması; ikincisi, iki ədalətli tərəf arasında əməli təfərrüatların mübahisəsiz vəziyyətdə təhlükəsizliyini təmin etməkdir.

Alqoritmin tətbiqatları, əsasən şifrələmədə, məsələn, SSL və TLS kimi protokollarda və ya VPN-lərdə görülür. Bundan əlavə, haqqında danışılan alqoritmi, kriptoanaliz və verilənlər mübadiləsi üçün də istifadə olunur.

Açar sözlər: Diffie-Helman alqoritmi, şifrələmə, asimmetrik şifrələmə, kriptoqrafiya, ictimai açar, mübadilə protokolları.

Giriş

Yalnız bir neçə insan, məlumatların ötürülmədikləri xüsusiyyətlərinə nəzər salaraq Diffie-Hellman alqoritminin mahiyyətini anlamağa cəsarət edir. Əsasən, çoxları bu anlayışa ehtiyac duymurlar. Ancaq, kompüter sistemlərinin istifadəçiləri üçün, bu anlayışa sahib olmaq maraqlı və zərər verməyəcək bir şeydir. Bilhəddə, Diffie-Hellman alqoritminin açar mübadiləsi, informasiya təhlükəsizliyi və kriptoqrafiya ilə məşğul olanlar üçün əhəmiyyətlidir.

Əgər Diffie-Hellman alqoritminin texniki və riyazi detallarına daxil olmasaq, onun mənasını bu cür izah edə bilərik: bu alqoritm, məlumatların şifrələnərək ötürülməsi prosesində iştirak edən kompüter və ya sistemlər arasında istifadə olunan bir şifrələmə və şifrələnmə metodu kimi təsəvvür edilə bilər.

Diffie-Hellman alqoritminin ən əsas xüsusiyyətlərindən biri, məlumatların ötürüldüyü kanalın qorunmadığı halda belə, onların müdaxiləsizliyini təmin etməsidir. Həmçinin, bu alqoritmin istifadəsi zamanı, əsas mübadiləni həyata keçirən kanal da qorunmağa davam edir.

Bu alqoritmin yaranması 1976-cı ildə baş vermişdir və Whitfield Diffie və Martin Hellman tərəfindən başlatılmışdır. Ralph Merkle isə bu işə tez edilmişdər və şifrələnmə metodlarının təhlükəsizliyini təmin etmək üçün ictimai paylaşım sistemlərini araşdırmaqla məşğul olmuşdur.

Ən sadə şəkildə izah edəndə, bu alqoritm, kriptoqrafiya texnologiyalarına əsaslanan test özəlliklərindən biridir və bu sahədəki mütəxəssisləri belə təəccübləndirir. Həqiqətən, şifrələrin ədəbiyyatı geniş tarixə malikdir. Bütün məsələ, e-poçt və ya proqramlar vasitəsilə məlumatların mübadiləsinə kömək edən iki abunəçinin var olmasıdır. Lakin bəhs etdiyimiz alqoritmi, bu məlumatların şifrələnmə açarlarının iki tərəfə daxil olmasını tələb edir. Beləliklə, onların təsadüfi rəqəmləri də eyni olmalıdır.

Əvvəlcə, Diffie-Hellman alqoritmi, şifrələnmə və şifrələnmədən asılı olaraq məlumatların təhlükəsiz mübadiləsinə imkan verən kriptoqrafiya alqoritmidir. Bu alqoritmin əsas fikri, açıq və gizli açarlar vasitəsilə təhlükəsiz məlumat mübadiləsini həyata keçirməkdir.

Alqoritmin əsas prinsipi, iki istifadəçi arasında təhlükəsiz bir qəbul əsasının yaradılmasına imkan verən bir protokoldur. Bu, ictimai açarın bir sənədin şifrələnməsi və açılmasına imkan verir. İki istifadəçi arasında təhlükəsiz bir əlaqə qurmaq üçün ictimai açarlarını mübadilə edirlər, lakin gizli açarı ictimai olmayan bir şəkildə saxlayırlar.

Diffie-Hellman alqoritmi, əsasən yüksək təhlükəsizlik səviyyəsi ilə tanınır və kriptoqrafiyanın ən əsas tətbiqlərindən biridir. Bu alqoritmin əsas gücü, məlumatların ictimai açarların vasitəsilə mübadilə edilməsindən qorunmağı və bu mübadilənin təhlükəsiz olmasını təmin etməsidir.

Bununla birlikdə, məşhur olan bu alqoritminin də qəribə tərəfləri var. Bir müddət əvvəl, bilim adamları alqoritmin kömək edə biləcəyi təhlükəsizlik açıqları ilə maraqlanırdılar. Ancaq, bu təhlükəsizlik açıqları sonradan kapatıldı və alqoritmin güvənlilik səviyyəsi artırıldı.

Ümumiyyətlə, Diffie-Hellman alqoritmi kriptoqrafiya dünyasında əhəmiyyətli bir rol oynayır və məlumatların təhlükəsiz mübadiləsini təmin etmək üçün effektiv bir alətdir.

Məqsəd

Alqoritmin əsas məqsədi, məlumatların sərfəli və təhlükəsiz bir şəkildə köçürülməsini təmin etmək deyil, həm də onların təhlükəsiz bir şəkildə əldə edilməsini sağlamaqdır. Buna görə də, bu növ bir transfer

sistemi bütün kommunikasiya kanallarında tam təhlükəsizlik təmin etməlidir. Məsələn, İkinci Dünya Müharibəsi illərində, müttəfiq ölkələr Enigma adlı şifrələmə maşını üçün avtomatlaşdırılmış bir şifrələmə mexanizmini istifadə edirdilər, və bu kodlar Morse kodu ilə ötürülürdü. Hazırda isə, belə bir sistem artıq nəhəng olsa da, hətta ən inkişaf etmiş kriptoqrafiya ekspertləri belə onun kodunu deşifrə edə bilmirlər. Yalnız bir dəfə şifrələnmiş olandan sonra Alman filosunun göndərdiyi mesajların açıq şifrəsi idi.

Metodlar

Diffie-Hellman alqoritmi, simmetrik şifrələmə sisteminə aid olduğu hesab olunan assimetrik şifrələmə protokolları əsasında yaranmışdır. Lakin, açarların hesablanması prosesində əsas aspektləri nəzərə alsaq, bir çox hallarda cəbrə geri qayıtmalıyıq. Bu baxımdan, hər iki istifadəçi təsadüfi ədədlər a və b yaradır. Əvvəlcədən, x və y dəyərlərinə malikdirlər, hətta istənilən proqrama "təyin olunmuş" ola bilərlər. Məsələn, bir mesaj göndərərkən və ya qəbul edərkən, A abunəçisi $A = x \bmod y$ əsas dəyərini hesablayır və ikinci B abunəçisi $B = x^b \bmod y$ kombinasiyasını, sonra şifrli açarın ilk istifadəçi tərəfindən istifadə edilir. Bu, birinci mərhələdir. Açıq-açarlı kriptoqrafiya anlayışı Whitfield Diffie, Martin Hellman tərəfindən 1976-də təqdim edilib.

Diffie-Hellman Açar Razılaşma Protokolu.

Diffie-Hellman açara razılaşma protokolu 2 tərəfə eyni açara razılaşmağa və mesajı bu açar vasitəsilə göndərməyə kömək edir. Bu protokol diskret logarifm probleminə əsaslanır. Bu protokol geniş istifadə edilən açara razılaşma protokoludur. Bəzi ədədlər nəzəriyyəsinə əsaslanır.

- a mod b = n burada hər hansı m üçün m : a=m*b+n
- Protokol 2 açıq parametrdən istifadə edir
- -generator g (adətən 160 bit uzunluğunda olur)
- - sadə ədəd p (adətən 1024 bit uzunluğunda olur)

Əgər Alice Bobla açara razılaşmaq istəyirsə rastgele seçilmiş rA rəqəmini generasiya edir. Daha sonra $t_A = g^{rA} \bmod p$ hesablayır və Bob-a göndərir. Bob da eyni şəkildə rastgele rB ədədini seçir və $t_B = g^{rB} \bmod p$ hesablayır və Alice-a göndərir. Daha sonra Alice $t_B^{rA} \bmod p$ hesablayır və Bob isə $t_A^{rB} \bmod p$ hesablayır. Bunların ikisi də $g^{rArB} \bmod p$ -ə bərabərdir, Bu bundan sonrakı danışıqlar üçün açar olaraq istifadə edilə bilər

Gördüyümüz kimi, A və B tərəflərinin hesabladığı dəyərlərə üçüncü tərəfin müdaxiləsi mümkün deyil, çünki ikinci mərhələdə ortaq əsasın necə hesablandığına dair məlumat olmalıdır.

Beləliklə, ictimai açarın hesablanması ilə əlaqədən qaldırıla bilər. Diffie-Hellman alqoritmasına baxdığımızda, nümunədən bir misal aşağıdakı kimidir:

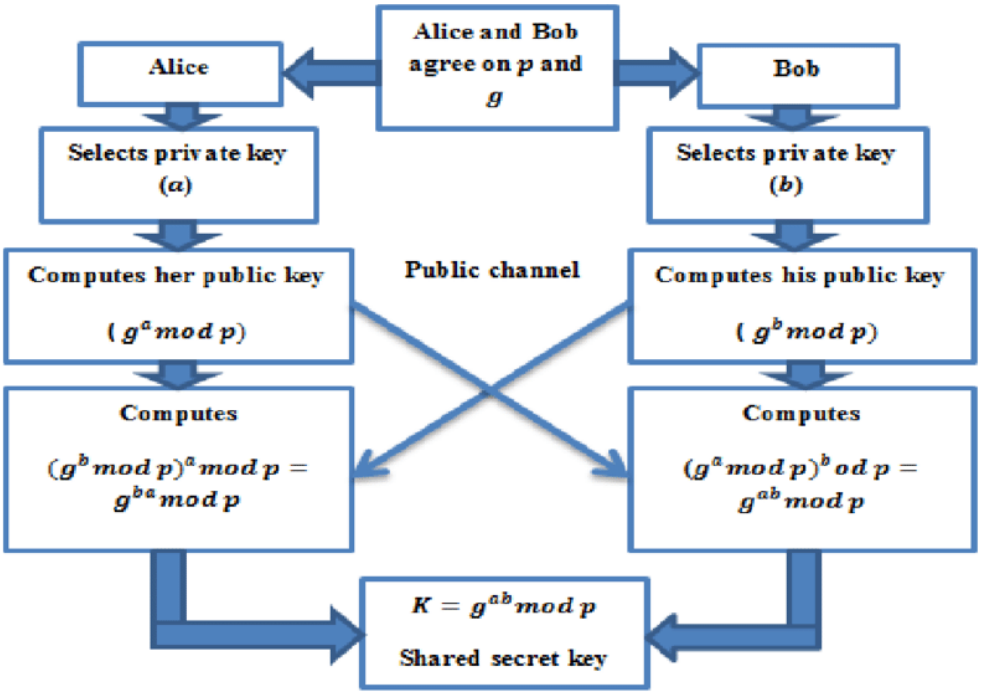
1) Birinci istifadəçi x-ə əsaslanan B modulunu hesablayır; $y = x^a \bmod y$;

2) Y-dən və başlangıca aid olan ədəddən ikinci B parametrinin şəbəkə protokolundan əldə edilmiş A əsasını təyin edir: $A^b \bmod y = x^{ab} \bmod y$.

Dərəcələrin bir-birinə uyğun olduğunu və nəticə dəyərlərinin eyni olduğunu görürük. Beləliklə, hər iki tərəf məlumatlarının açıq mənbələri, bir nöqtəyə qədər azaldıla bilər. Əgər müdaxilə şəraitində üçüncü tərəfin qarışdığını düşünsək, bu halda biz müntəzəm ədədlərdən (məsələn, 10^{100} və ya 10^{300}-dən) danışa bilərik.

Hazırda mövcud olan parol yaradıcıları və giriş kodlarının heç biri bu növ təhlükələri özündə daşıyır (məsələn, ötürmə sistemlərinə müdaxilə etmək üçün ara parametrləri təyin etmələri və s.). Bu, praktiki olaraq ələ keçirilməsi məqsədilə mümkün deyil. Lakin, bu növ bir təhlükəsizlik sisteminin boşluqları mövcuddur.Diffie-Hellman alqoritmi üzrə əsas paylaşma növü olan diskret logarifm bilik ilə əlaqəlidir. Belə bir bilik əgər mövcud olarsa, Diffie-Hellman alqoritmini deşifrə etmək mümkündür (xüsusilə, ilk və son parametrləri biləndə). Başqa bir dəyişlə, bu bir bilik kifayət qədər böyük olanda qorunma təhlükəsizlik açığına yol açar. Proqramlaşdırma dillərində Diffie-Helman alqoritminin istifadəsi

Java platformasında danışılan alqoritmi yalnız "müştəri-server" əlaqələrində istifadə olunur.
C platformasında Diffie-Hellman alqoritmi çox da səmərəli deyil. Bu, bəzi hallarda proqramlaşdırma dili əsasən özü əsas hesablamaları ilə işləyərkən və ya yüksəltildikdə (hətta tərtib edərkən) dəyərləri tam dəyərlərə və ya yuvarlamaq istənilənə uyğun deyil kimi problemlərlə üzləşməklə əlaqəlidir. Bu, xüsusilə int funksiyasının sui-istifadəsi ilə bağlıdır.
Müasir şifrələmə alqoritmləri arasında Diffie-Hellman alqoritminin hələlik aşılmadığı inanılır. Əslində, məlumat şifrələmə sahəsində tanınmış təhlükəsizlik sistemlərinin, məsələn, AES128 və AES256 kimi, ortaya çıxmasına kömək edən o idi. Ancaq təcrübələr göstərir ki, hər hansı bir insanın yaratmadığı nömrələr mövcud olsa belə, çox az sistem, hətta milyonlarla dəfə daha çox sayda olmasına baxmayaraq, yalnız ilk on (və ya daha çox) dəyərlərindən istifadə edir.



Şəkil. Diffie-Helman alqoritminin blok-sxemi

Nəticə

Nəticədə, deyə bilərik ki, ümumilikdə sistem və onun alqoritmik komponentləri aydınlaşdırıldı. Həmçinin aşkarladıq ki, Diffie-Helman alqoritminin indiyə qədər heç kim tərəfindən istifadə olunmayan böyük imkanları mövcuddur. Başqa bir tərəfdən isə, alqoritmin mənfi xüsusiyyətləri yaxud qüsurları vardır ki, bunların da nəticəsində istifadəçinin məlumatları şübhə altında qala bilir. Əlbəttə ki, hər bir şifrləmə metodunda olduğu kimi Diffie-Helman açar mübadiləsində də üçüncü tərəfin müdaxilə edə bilmə ehtimalı sıfıra bərabər deyil. Ümumiyyətlə, bu tipli məsələlərdə yaranan problemlərə belə bir yekun fikir bildirmək olar ki, əgər bir məlumatı şifrləmək mümkündürsə, deməli deşifrləmək də mümkündür. Buradakı əsas predmet, metodun, ümumiyyətlə, deşifrə edilə bilməməsi deyil, çətin çözülə bilməsidir.

Ədəbiyyat

[1] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
[2] Merkle, R. C. (1978). Secure communications over insecure channels. Communications of the ACM, 21(4), 294-299.
[3] Stinson, D. R. (2006). Cryptography: Theory and Practice (3rd ed.). CRC Press.
[4] Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
[5] Katz, J., & Lindell, Y. (2015). Introduction to Modern Cryptography (2nd ed.). Chapman and Hall/CRC.
[6] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
[7] Boneh, D., & Shoup, V. (2000). A Graduate Course in Applied Cryptography.
[8] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
[9] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.
[10] Goldreich, O. (2001). Foundations of Cryptography: Basic Applications (Vol. 2). Cambridge University Press.
[11] Mao, W. (2003). Modern Cryptography: Theory and Practice. Prentice Hall PTR.
[12] Lindell, Y., & Katz, J. (2007). Secure Multiparty Computation and Secret Sharing. Cambridge University Press.
[13] Diffie, W., & Landau, S. (2008). Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press.
[14] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2012). Post-Quantum Cryptography. Springer.
[15] Smart, N. P. (2003). Cryptography: An Introduction (2nd ed.). McGraw-Hill Education.

AÇIQ MƏNBƏLİ İNFORMASİYA MÜBADİLƏ SİSTEMLƏRİNİN MÜQAYİSƏLİ TƏHLİLİ

Sultanova Axirə
Yediyarov Xəyal
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə
Bu məqalə mesaj mübadiləsi sistemlərində istifadə edilən iki açıq mənbəli proqram təminatını müqayisə edir: Apache Kafka və RabbitMQ. Bu alətlər, şifrələmə və Java platformasındakı tətbiqlərlə birbaşa işləyə bilmə, yəni Java API-lərini təmin etmə kriteriyalarını, eyni zamanda Secure Sockets Layer/Transport Layer Security (SSL/TLS) protokollarını dəstəkləyir. Bu tədqiqatı aparmaq üçün diqqət mərkəzi performans analizi olan mühit yaradılaraq istifadə edilmişdir.

Açar sözlər: açıq mənbəli sistemlər, Apache Kafka, RabbitMQ, asinxron növbələr, Publish&Subscribe, RPC, məlumat axını

Giriş.
Informasiya texnologiyalarının (IT) artan istifadəsi ilə birlikdə kommunikasiyanın həcmi də artır, bu da informasiya alış-verişlərinin əlaqələndirilməsi və standartlaşdırılmasını, həmçinin xüsusi ara bağlantı