ISSN 2181-3187

MULTIMEDIALI ALOQA TARMOQLARIDA AXBOROTNI XAVFSIZLIGI

Irgasheva Durdona Yakubdjanovna
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kiberxavfsizlik fakulteti, dekani, dotsent
Shaydullayev Jahongir Qudrat òğli
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kiberxavfsizlik fakulteti magistranti

Annontatsiya: Ushbu maqolada Multimediali aloqa tarmoqlarida axborotni xavfsizligi, ma'lumotlar yaxlitligi va autentifikatsiya haqida fikr yuritilgan.
Kalit so'zlar: maxfiylik, ma'lumotlar yaxlitligi va autentifikatsiya.

Internetda raqamli aloqa shaklining ko'payishi bilan birga multimedia ma'lumotlarining xavfsizligi tobora muhim ahamiyat kasb etmoqda. Har xil turdagi ilovalarda keng assortimentdagi rasm va videolardan foydalanish bugungi kunda xavfsizlik va maxfiylik masalalariga katta e'tibor qaratmoqda. Multimedia ma'lumotlarini shifrlash tranzit yoki saqlashda maxfiy ma'lumotlarning kiruvchi va ruxsatsiz oshkor etilishining oldini olishga yordam beradi.

Multimedia axborot xavfsizligiga kelsak, kriptografiyaning uchta asosiy maqsadi mavjud, ya'ni. maxfiylik, ma'lumotlar yaxlitligi va autentifikatsiya. AES va Rijndael shifrlash algoritmlari bir-birining o'rnida ishlatilgan bo'lsa-da, ular hali ham bitta farqga ega, qo'llab-quvvatlanadigan qiymatlar diapazoni va shifr kaliti uzunligi. Rijndael - bu o'zgaruvchan blok va kalit uzunligiga ega bo'lgan blokli shifr. Blok uzunligi va kalit uzunligi 32 bitning ko'paytmasi va 128 dan 256 bitgacha bo'lgan qiymatga ega bo'lsa, mustaqil ravishda belgilanishi mumkin. Rijndael versiyasi kattaroq blok yoki kalit uzunligiga ega ekanligi aniqlanishi mumkin bo'lsa-da, hozirda uni talab qilish ehtimoli yo'q. AES blok uzunligini 128 bitni aniqlaydi va faqat qo'llab-quvvatlanadigan kalit uzunliklari 128, 192 va 256. Rijndaeldagi qo'shimcha blok va kalit uzunligi AES tanlashda e'tiborga olinmagan, shuning uchun ular joriy FIPS standartida ham ishlatilmaydi.

Kompyuter va Internet texnologiyalarining rivojlanishi bilan multimedia ma'lumotlaridan foydalanish tez sur'atlar bilan o'sib bormoqda. Shunday qilib, maxfiy ma'lumotlarni uzatish yoki tarqatishdan oldin ularni himoya qilish zarurati yuqori. Shunday qilib, ushbu tezisda multimedia kontentini shifrlash usuli bilan himoya qilishga yordam beruvchi Rijndael algoritmi o'rganilib, o'rganilgan material asosida nazariy hisobot yoziladi.

Onlayn-televideniye, videokonferentsiya, davlat (tibbiy, harbiy) raqamli xizmatlar kabi deyarli barcha raqamli xizmatlar ma'lumotlarni saqlash va uzatishda

ISSN 2181-3187

(audio/video) kuchli xavfsizlikni talab qiladi. Bugungi kunda jadal rivojlanayotgan raqamli dunyoda internet juda katta tezlikda o'sib bormoqda, shuning uchun ma'lumotlar xavfsizligi tobora muhim ahamiyat kasb etmoqda. So'nggi yillarda tobora ko'proq iste'molchi elektron xizmatlari (mobil va PDA) multimedia xabarlarini saqlash va almashish funksiyalarini qo'shishni boshladi.

Jamiyatimizda texnologiyaning rivojlanishi tufayli raqamli tasvirlar va videolar oddiy va oddiy matndan ko'ra katta rol o'ynaydi, shuning uchun foydalanuvchi maxfiyligini jiddiy himoya qilishni talab qiladi. Hamma narsani xavfsiz qilish uchun audio va videolarni shifrlash juda muhim hujumlardir, chunki bu ruxsat etilmagan shaxslarning zararli ta'sirini kamaytirishga yordam beradi. Ilm-fan va texnologiyaning, asosan, kompyuter va aloqa sanoatidagi so'nggi yutuqlari raqamli multimedia kontentini Internet orqali tarqatish uchun potentsial katta bozorga imkon beradi. Biroq, raqamli hujjatlarning, multimedia ishlov berish vositalarining tez o'sishi va butun dunyo bo'ylab Internetga kirishning mavjudligi mualliflik huquqini firibgarlik va multimedia kontentini nazoratsiz tarqatish uchun mukammal muhitni tug'dirdi. Hozirgi vaqtda asosiy muammolardan biri multimedia tarmoqlarida intellektual kontentni himoya qilishdir.

Texnik muammolarni hal qilish uchun ikkita asosiy xavfsizlik texnologiyasi ishlab chiqilmoqda:

1. Multimedia shifrlash texnologiyasi raqamli kontent juda ko'p sonli tarqatish tizimlarida tarqatilayotganda oxirigacha xavfsizlikni ta'minlaydi.
2. Mualliflik huquqining firibgarligi, egalik izi va autentifikatsiyani oldini olish uchun suv belgilari texnologiyasi qo'llaniladi.

Maxfiylik shaxsiy ma'lumotlarni ruxsatsiz kirishdan himoya qilishni anglatadi. Dushman deb nomlanuvchi kiruvchi tomon materialga kira olmasligi kerak. Ma'lumotlarning yaxlitligi ma'lumotlarning hech qanday istalmagan tarzda o'zgartirilmaganligiga ishonch hosil qiladi. Shuning uchun autentifikatsiya usullari ikki guruhda o'rganiladi:

1. Shaxsning autentifikatsiyasi Shaxsning autentifikatsiyasi xabarni qabul qiluvchining jo‘natuvchining identifikatorini va uzatish vaqtida uning faol ishtirokini olishiga ishonch hosil qiladi.

2. Xabarning autentifikatsiyasi Xabarning autentifikatsiyasi xabar jo'natuvchining identifikatorini tekshirishni ta'minlaydi. Bundan tashqari, agar u uzatish davrida o'zgartirilsa, jo'natuvchi xabarning muallifi bo'lmasa, ma'lumotlar yaxlitligini tasdiqlovchi barcha dalillarga ega.

Kriptografiya multimedia kontentini himoya qilishning muhim vositasidir. Barcha multimedia fayllari internet orqali tarqatilgunga qadar shifrlangan. Fayl shifrlanganligi sababli, kalitlarga kirish imkoni bo'lmagan barcha odamlar uchun bu foydasiz. Shunday qilib, kontentni shifrlash kaliti kontent provayderidan boshqa hech

ISSN 2181-3187

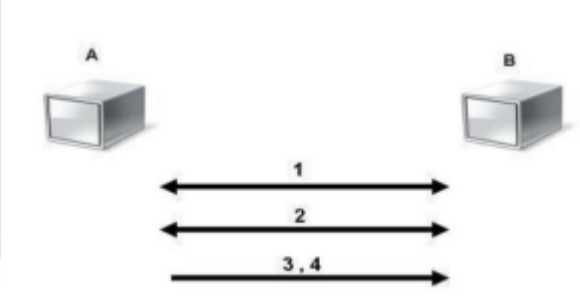
kimga oshkor etilmasligi kerak. Shifrlash - bu ma'lumotni hech qanday tajovuzkor tanib bo'lmaydigan shaklga o'zgartirish orqali keraksiz hujumlardan himoya qilish usuli. Ma'lumotlarni shifrlash asosan matn, tasvir, audio va boshqalar kabi ma'lumotlarni o'zgartirishdir. translyatsiya paytida o'qib bo'lmaydigan, ko'rinmas yoki o'tkazib bo'lmaydigan bo'lishi uchun. Shunday qilib, asl ma'lumotlarni qayta tiklash uchun qabul qiluvchi ma'lumotlarni shifrlash deb nomlanuvchi ma'lumotlarni shifrlashni o'zgartiradi.

Shifrlash jarayoni quyidagicha ta'riflanishi mumkin C = E (P, K)
Bu erda, P = Asl ma'lumotlar
E = Shifrlash algoritmi
K = Shifrlash kaliti
C = uzatiladigan va hujumga duchor bo'lishi mumkin bo'lgan shifrlash xabari.
P= D (C, K)Bu yerda,
C = Shifrlangan xabar;
D= shifrni ochish algoritmi
K= shifrni ochish kaliti;
P = Qayta tiklangan ma'lumotlar

1970 yilgacha ishlab chiqilgan barcha klassik kriptotizimlar simmetrik kalitli kriptotizimlarga misol bo'la oladi. Bundan tashqari, 1970 yildan keyin ishlab chiqilgan kriptotizimlarning aksariyati simmetrikdir. Zamonaviy simmetrik kalitlarga juda mashhur misollar qatoriga quyidagilar kiradi:

1. AES (Kengaytirilgan shifrlash standarti)
2. DES (Ma'lumotlarni shifrlash standarti)

Barcha simmetrik kalitlar umumiy manfaatlarga ega, ular muloqot qiluvchi tomonlar o'rtasida taqsimlangan sirga bog'liq. Sirdan ham shifrlash, ham shifrni ochish kaliti sifatida foydalanish mumkin. Simmetrik kalitning kamchiligi shundaki, u katta aloqa tarmog'ini boshqara olmaydi. Boshqa tomondan, nosimmetrik kalit ochiq kalit kriptotizimlari bilan bir xil xavfsizlik darajasi uchun kichikroq hajmni talab qiladi, bu esa aloqani tezlashtiradi va xotirani kichikroq qiladi.

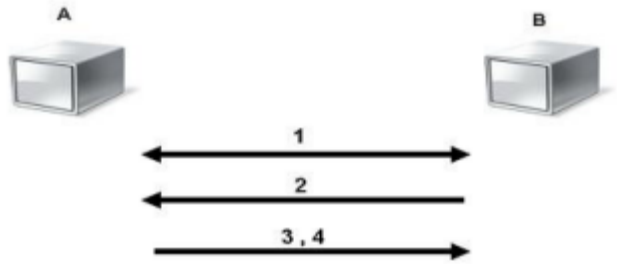


1-rasm Simmetrik shifrlash

ISSN 2181-3187

1. A va B kriptotizimlar haqida kelishib oladilar.
2. A va B foydalaniladigan kalit haqida kelishib oladilar.
3. Umumiy kalit yordamida shifrlangan xabar.
4. B umumiy kalit yordamida shifrlangan xabarning shifrini ochadi.

Ushbu turdagi kriptotizimlarda ikkita alohida kalit mavjud: ochiq kalit, ochiq kalit va faqat egasiga ma'lum bo'lgan maxfiy kalit. Ushbu turdagi tizim shifrni ochish va shifrlash uchun boshqa kalitdan (ommaviy va shaxsiy kalit) foydalanish sababli "assimetrik" deb nomlanadi. Ma'lumotlar ochiq kalit yordamida shifrlangan va uni faqat shaxsiy kalit yordamida hal qilish mumkin



2-rasm Assimetrik shifrlash

1. A va B kriptotizimlar haqida kelishib oladilar.
2. B ochiq kalitni A ga yuboradi.
3. A kelishilgan shifr va B ning ochiq kaliti yordamida xabarni shifrlaydi.
4. B o'zining shaxsiy kaliti va kelishilgan shifrdan foydalangan holda shifrlangan xabarning shifrini ochadi.

Multimedia shifrlash texnologiyasi birinchi marta 1980 yilda taqdim etilgan va 90-yillarning o'rtalarida tadqiqot uchun dolzarb mavzuga aylandi. Uning rivojlanishini uch bosqichga bo'lish mumkin; xom ma'lumotlarni shifrlash, siqilgan ma'lumotlarni shifrlash va qisman shifrlash.

90-yillarga qadar faqat bir nechta multimedia kodlash usullari standartlashtirildi. Ko'pgina multimedia ma'lumotlari (tasvir, video) xom shaklda uzatilgan yoki saqlangan. Multimedia shifrlash, asosan, pikselni almashtirish yoki skrambllashga asoslangan edi, ya'ni video/tasvir o'zgartirilib, natijada olingan ma'lumotlar tushunarsiz bo'ladi. Masalan, bo'sh joyni to'ldirish egri chiziqlari tasvir/video ma'lumotlarini o'zgartirish uchun ishlatiladi, bu esa qo'shni tasvirlar/video piksellar o'rtasidagi munosabatni chalkashtirib yuboradi. Evropa televizion tarmoqlari signallarni shifrlash uchun Eurocrypt standartidan foydalanadi, bu esa maydonni satr bo'yicha o'zgartiradi.

ISSN 2181-3187

Ushbu usullar hisoblashning murakkabligi va narxi pastligi sababli qo'llaniladi. Shunga qaramay, ushbu turdagi modifikatsiya qo'shni piksellar o'rtasidagi munosabatni o'zgartiradi, bu esa siqish operatsiyasini ishlamaydi. Shuning uchun, bu shifrlash algoritmlari faqat siqishni talab qilmaydigan dastur uchun foydalidir.

1990-yillarning boshlarida multimediya texnologiyasining rivojlanishi bilan JPEG, MPEG va boshqalar kabi tasvir va audio/video kodlashning ba’zi standartlari ishlab chiqildi. Umuman olganda, bu turdagi multimedia ma’lumotlari saqlash yoki uzatishdan oldin siqiladi, bu esa xom ma’lumotlarni shifrlash uchun mos emas. ushbu ilova uchun.

1990-yillarning oxirlarida internet texnologiyasi rivojlanganidan keyin yaratilgan multimedia ilovasi real vaqt rejimida ko‘proq ishlashni va o‘zaro ta’sir qilishni talab qildi. Ma'lumotlarning faqat ma'lum qismlarini shifrlash orqali shifrlash samaradorligini oshirish orqali yakuniy shifrlangan fayl hajmini kamaytirish mumkin. Tarmoqning jadal rivojlanishi tufayli maxfiylik va maxfiylikni himoya qilish uchun axborot xavfsizligini takomillashtirish muhim ahamiyatga ega. Shifrlash algoritmlari axborot xavfsizligini ta'minlashda muhim rol o'ynaydi. Ma'lumotlarni shifrlash va shifrini ochish uchun turli xil algoritmlar AES, DES ishlatiladi.

Eng ko'p ishlatiladigan shifrlash algoritmlariga AES va DES kiradi. Ushbu algoritmlardan AES yoki DES algoritmlari yordamida shifrlanishi yoki shifrlanishi mumkin bo'lgan ma'lumotlar faylini yaratish orqali katta hajmdagi ma'lumotlarni himoya qilishni istagan kishi foydalanishi mumkin.

Ashwin Kumar va K.S tomonidan AES, DES va Blowfish o'rtasida taqqoslash mavjud edi. Sandha xavfsizlik va quvvat iste'moli nuqtai nazaridan va ular AES boshqa algoritmlarga qaraganda yaxshiroq ishlashga ega degan xulosaga kelishdi. AES va DES o'rtasida yaxshiroq vaqt bilan xavfsizroq kontentni taqdim etishda qaysi biri yaxshiroq ekanligi haqida ko'proq taqqoslash mavjud. Ular, shuningdek, ikkala algoritm ham mashinaga qarab har xil vaqt talab qilishini ko'rsatadi.

Ma'lumotlarning butun fayllarini shifrlash katta hajmdagi ma'lumotlarni himoya qilishning amaliy usuli bo'lishi mumkin. Biroq, fayllarni ommaviy shifrlash samarasiz va katta hajmli bo'lishi mumkin, chunki fayldagi shifrlangan ma'lumotlarning tanlangan qismiga kirish mumkin emas. Ilova ma'lumotlarning faqat ma'lum bir qismiga kirishi kerak bo'lsa ham, butun faylni shifrlash kerak. Faylning bir qismini shifrlash imkoniyati bo'lmasa, turli xil ilovalarga ma'lumotlarga kirishning boshqa darajasini ta'minlay oladigan ma'lumotlarni qayta ishlash tizimini loyihalash qiyin.

Foydalanilgan adabiyotlar ro’yxati;

1. Borka Jerman-Blazic, Tomaz Klobucar, 2002. Advanced Communications and Multimedia Security. New York: Springer Science+Business Media New York.
2. Ching-Yung Lin, 2006. Topics in Signal Processing -- Multimedia Security Systems. [Online] Available at:

ISSN 2181-3187

http://www.ee.columbia.edu/~cylin/course/mss/MSS_notes.html [Accessed 1 10 2015].

3. Emanuil Rednic; Andrei Toma, n.d. Software Analysis. SECURITY MANAGEMENT IN A MULTIMEDIA SYSTEM, 4(2), pp. 237-247.
4. Pande, J. Zambreno, 2013. Advances in Multimedia Encryption. In: Embedded Multimedia Security Systems. London: Springer-Verlag, pp. 11-22. [Online] Available at: http://www.springer.com/cda/content/document/cda_downloaddocument/9781447144588- c2.pdf?SGWID=0-0-45-1345406-p174549534 [Accessed 11 10 2015].
5. Saha Arunabh n.d. Overview of Multimedia Security, s.l.: s.n. [Online] Avaiable at: http://www.academia.edu/8199308/Overview_of_Multimedia_Security [Accessed 15 11 2015].