|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sana:** |  |  |  |  |
| **Sinf:** | **11-A** | **11-B** | **11-V** | **11-G** |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Mavzu:** Internetda saqlanayotgan axborot manbalarining xavfsizligi muammolari

 ***Adxamjon\_Vahobov +99890 300 02 21 @rishton7***

**Fan: Informatika № 30**

**Darsning maqsadi:**

##### **Ta’limiy:** O’quvchilarga internetda saqlanayotgan axborot manbalarining xavfsizligi muammolarini o’rgatish va tushuntirish.

**Rivojlantiruvchi:** O’quvchilarni mustaqil fikrlarini oshirish va rivojlantirish.

**Tarbiyaviy:** Vatanini sevish, milliy va umuminsoniy qadriyatlarga hurmatda bo‘lish, odob-axloq qoidalariga rioya qilishni singdirish.

**Tayanch va fanga oid kompetensiyalar:**

***TK:*** *ishlash, saqlash, ulardan foydalana olish, ularning xavfsizligini ta’minlash, mediamadaniyatga ega bo‘lish.*

***FK:*** *axborot xavfsizligini ta’minlaydigan usullardan foydalanib axborot uzata oladi; matn va jadval protsessorlari, taqdimot dasturlari yordamida hujjatlarni pochta orqali uzata oladi;*

**Dars usuli:**  suhbat, tushuntirish, “Savol-javob” metodi, “Rasmli boshqotirma” , “To‘g‘risini top”,”Yosh aktyor”o‘yinlari.

**Dars turi: Yangi bilim berish.**

**O’quv jarayonining amaliga oshirish texnologiyasi:**

O’qitish usullari: blits-so’rov, savol-javob.

O’qitish shakllari: guruhlara ishlash, frontal, jamoaviy.

O’qitish vositalari:11-sinf darsligi, mavzuga oid dars taqdimoti,

Monitoring va baholash: og’zaki va test nazorati, amaliy vazifalar.

**Darsning borishi:**

1. **Tashkiliy qism:**

O’quvchilar bilan salomlashish

Xonani va o’quvchilarni darsga tayyorliklarini kuzatish

Yo’qlamani aniqlash

Navbatchi axboroti.

Siyosiy daqiqa.

1. Darsning maqsad va vazifalarini qo’yish.
2. Tayanch bilimlarning faollashtirish.

Uyga vazifalarini tekshirish va o’tilgan mavzuni mustahkamlash.

1550-yilda o‘quvchilarga kub tenglamani yechish yoclini birinchi bo‘lib aniqlagan italyan matematigi Djerolamo Kardano “De subtilitate libri xxi” risolasida trafaret deb nomlangan shifrlash usulini e’lon qildi. Bu usulga ko‘ra maxfiy matn biror kattaroq oddiy mazmunli maktubni ichiga joylashti- rilib jo‘natiladi. Maktubni ustiga ma’lum bir qonuniyatda yasalgan Kardano trafareti yotqiziladi, natijada maxfiy xabar ochiladi.

1. **Dars materiallarini tushuntirish (materiallarni tushuntirish dars prezentatsiyasi va videorolik, amaliy harakatlar, tayyor ishlar ko’rgazmasini namoyish qilish bilan birgalikda olib boriladi).**

**Nazariy qism:**

Internet tizimi orqali moliyaviy harakatlami amalga oshirish, tovar-boy- lik va xizmatlami buyurtmalash, plastik kartochkalarni qo‘llash, masofaviy muloqotni amalga oshirish va boshqa imkoniyatlardan foydalanish, o‘z nav- batida, axborot xavfsizligini ta’minlashni ham talab qiladi. Internet tizimi orqali tarqatilayotgan har qanday ma’lumotlar hamma vaqt bir necha yo‘na- lishlar va serverlar orqali o‘tib kerakli manzilga yetib keladi. Ushbu yo‘na- lishlarda tizimdagi axborotlar yaxlitligi va daxlsizligiga turli tashqi tahdidlar bo‘lishi mumkin.

Umuman olganda, Internet tizimi har qanday axborot manbasiga cheklov- siz murojaat qilish imkoniyatini ta’minlashdir. Axborot xavfsizligi muammo- si esa, ma’lum darajada ma’lumotlardan foydalanishdagi cheklovlar tizimiga olib keladi. Lekin kriptografiya usullari yordamida foydalanuvchilar imkoni- yatlarini cheklamay ma’lumotlami himoya qilish mumkin.

Kriptografiya usullari asosida axborotni maxfiylashtirish shifrlash algoritmi yotadi. Lekin boshlang‘ich ma’lumotga qaytish uchun, shifr­lash algoritmini aniqlash kaliti zarur. Shunday qilib, algoritm va kalit kriptografiyaning asosiy tushunchasidir.

Simmetrik shifrlash algoritmlari foydalanuvchilar uchun ma’lum deb hisoblanadi. Axborot xavfsizligining asosida simmetrik kalitlar maxfiyligi darajasi yotadi. Berilgan shifrlash algoritmi uchun kalitning variantlari soni bilan xavfsizlik darajasi baholanadi.

Hozirgi paytga kelib simmetrik yopiq kalit bilan shifrlashning birmun- cha kamchiliklari namoyon bo‘lmoqda. Maxfiylik saqlangan holda ma’lumot jo‘natuvchi va qabul qiluvchi uchun kalitlami hosil qilish, saqlash va kerakli manzilga yetkazishda murakkabliklar pay do bo‘lmoqda. Masalan, bank tizi­mida moliyaviy faoliyat yurituvchi mijozlar soni juda ko‘p bo‘lganligidan, ulaming har birini alohida yashirin kalit bilan ta’minlash amalda mumkin emas. Shu sababli axborot xavfsizligini ta’minlashda asimmetrik kalitlaming afzalliklari ma’lum bo‘lmoqda.

Asimmetrik kalit usulida ma’lumot jo‘natuvchi ochiq kalit bilan axbo rotni shifrlaydi, qabul qiluvchi esa yopiq kalit yordamida faylni deshifrlaydi (yashirin ma’lumotni ochadi).

Simmetrik shifrlash usulidagi kamchiliklardan xoli, amerikalik olimlar R. Rivest, A. Shamir va L. Adelman tomonidan kashf etilgan RSA asim- metrik kalitlar asosidagi shifrlash usuli hozirgi paytda keng tarqalgan. Bank tizimida keng qo‘llaniladigan elektron imzoning maxfiyligini ta’minlash RSA usuliga yaqin usullar zimmasiga yuklatilgan.

RSA usuli bo‘yicha kalitlami hosil qilish algoritmi:

1. pvaq o‘zaro teng bo‘lmagan tub sonlar tanlab olinadi;
2. n=p\*q modul hisoblanadi;
3. n=(p-\){q-\) hisoblanadi;
4. 1 <d<n tengsizlikni qanoatlantiruvchi va n soni bilan o‘zaro tub bo‘l- gan e aniqlanadi;
5. Yashirin d soni (d\*e) mod n=1 tenglamani qanoatlantiruvchi qilib tanlab olinadi;

Shunday qilib, {e, n) - ochiq va (d, n) - yopiq kalitlar juftligini hosil qildik. RSA usuli bilan shifrlash va deshifrlash.

Matnni (e, n) ochiq kalit bilan shifrlash uchun:

* shifrlanayotgan matnni M(i) = 0,1,2,..., n-1, bloklarga ajratib olamiz;
* matn bo‘lagi M(i) ni C(i)=(M(i)e) mod n formula asosida shifrlaymiz;
* shifrlangan matn bo‘lagi C(z) ni yopiq kalit (d,n) yordamida M(i)=(C(i) d) mod n formula asosida deshifrlab boshlang‘ich matnni hosil qilamiz.
* Yopiq kalitlami ochish hal qilib bo‘lmas muammoga aylanishi uchun:
* 1. Ikkita juda katta tub sonlar (masalan har biri 1024 bitdan iborat) ni bir-biridan juda ham uzoq yoki yaqin qilmasdan tanlab olish zarur bo‘ladi;
* 2. (p-\)(p-l) va (q-X){q-X) sonlaming eng katta umumiy bo‘luvchilari mumkin qadar yaqin bo‘lishi zarur;
* 3. Odatda e soni sifatida Fermaning tub sonlari: 17, 257, 65537, ... olinadi;
* 4. Yopiq kalit maxfiy saqlanishi zarur.

**1-mashq.**

* p=3 va q=\ 1 sonlami tanlab olamiz;
* n= 3 • 11=33 sonni aniqlaymiz;
* (р-1) • (q-1)=20. Demak, shartga ko‘ra, masalan e=7;
* (d-1) mod 20=1 shartni qanoatlantirsak, d= 3 son hosil bo‘ladi;
* Lotin alifbosi harflarini 0 dan 26 gacha bo‘lgan tartibda raqamlab olamiz: A =1, V=2, S= 3;
* matnni ochiq (7,33) kalit bilan shifrlaymiz;

. C(l) = (37) mod 33 = 2187 mod 33 = 9;

. C( 2) = (17) mod 33 = 1 mod 33 = 1;

. C(3)= (27) mod 33 = 128 mod 33 = 29.

* Yopiq (3,33) kalitdan foydalanib shifrni ochamiz:

. M(l)=(93) mod 33 =729 mod 33 = 3

. M( 2)=(13) mod 33 =1 mod 33 = 1 ->A;

* M(3)=(293) mod 33 = 24389 mod 33 = 2-+V.
* 1977-yili mashhur yozuvchi va aniq fanlaming jonkuyari Martin Gardner Scientific American jumalida qiziqarli matematika bo‘yicha risolasini “Osh­kor etish uchun million yil ketuvchi mutlaqo yangi shifr” deb nomladi. Shifr­lash usulini ko‘rsatib, ochiq kalit uchun n ning qiymatini ham taqdim qildi: n = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541.
* n sonni tub sonlarga ajratgan insonlarga pul mukofoti va’da qildi. Qo‘shimcha savollar bo‘yicha Massachuset texnologiya instituti xodimlari R.Rivest, A.Shamir va L.Adelmanga murojaat qilishlari mumkinligini bildir- di. n kalit va shifrlangan matnni ham e’lon qildi.
* Ushbu muammoni hal qilish uchun 600 kishi hamkorlikda 17 yil ishlash- lariga to‘g‘ri keldi. Natijada
* p = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533
* q = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577 tub sonlari aniqlandi va shifr oshkor etildi.
* Shunday qilib, RSA usulining misli ko‘rilmagan kriptoustuvorligi isbot etildi. Yuqorida 64 va 65 xonalik tub sonlar ishlatilgan. Demak, juda kat- ta sonlar bilan ish ko‘rilgandagina RSA usulining elektron raqamli imzoni shakllantirishda ustivorligi yuqori bo‘ladi.

Elektron raqamli imzo (ERI) - elektron hujjatdagi mazkur elektron hujjat
axborotini ERIning yopiq kalitidan foydalangan holda maxsus o‘zgartirish
natijasida hosil qilingan hamda ERIning ochiq kaliti yordamida elektron huj-
jatdagi axborotda xatolik yo‘qligini aniqlashdan iborat

1. **Amaliy ish:**



1. Simmetrik shifrlash usullarining maxfiylik mezoni nimadan iborat?
2. RSA usuli bo‘yicha kalitlami hosil qilish algoritmini tushuntiring.
3. **Darsga yakun yasash:**

O’quvchilarni olgan bilimlari hamda qilgan ishlarini nazorat qilib baholash, ularni yo’l qo’ygan kamchiliklarini to’g’irlash.

1. **Uyga vazifa berish**: Ingliz tilidagi harflarini 1 dan 26 tartibda raqamlab, “million”, “secret”, “azamat” so’zlarini RSA usuli yordamida shifrlang va deshifrlang

**O’IBDO’:** \_\_\_\_\_\_\_\_\_\_\_\_ **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 *(imzo) (F.I.SH.)*