TOSHKENT AMALIY FANLAR UNIVERSITETI

HOMIDOV HAMDAM HASAN O‘G‘LI

Mavzu: Kriptografiyaning asosiy tushunchalari.

Mutaxassislik:

Agar siz o'rganishga tayyor bo'lmasangiz, sizga hech kim yordam berolmaydi. Agar siz o'rganishga tayyor bo'lsangiz, sizni hech kim to'xtata olmaydi

Kriptografiyaning asosiy tushunchalari.

Kriptografiya (yunoncha κρυπτός (kryptós) - "**mahfiy**," γράφω (gráfo) - **"yozish"** so‘zlaridan tashkil topgan) ochiq ma’lumotlarni shifrlashni, mahfiylashtirish usullarini o‘rganadi. Mahfiy matnni begona, bexabar kishilar tushunmasligi uchun yozuvni o‘zgartirish tizimi, bunda oldindan kelishilgan vositalardan — belgilardan foydalaniladi. K. diplomatik, harbiy, savdo-sotiq va moliyaga oid hamda diniy va boshqa matnlarni shifrlash uchun ishlatiladi. Bu yozuvning ko‘p turlari mavjud: matn harflarini raqamlar bilan almashtirish, harflar o‘rniga har xil shartli belgilar, matnda qo‘llanishi). lozim bo‘lgan harflar o‘rniga boshqa alifbo harflarini qo‘yib yozish va boshqa Kriptografik yozuv maxsus shifr yordamida o‘qiladi; 2) paleografiyaning maxfiy yozuv tizimi grafikasini o‘rganuvchi tarmog‘i.

Kriptografiyaning asosiy tushunchalari.

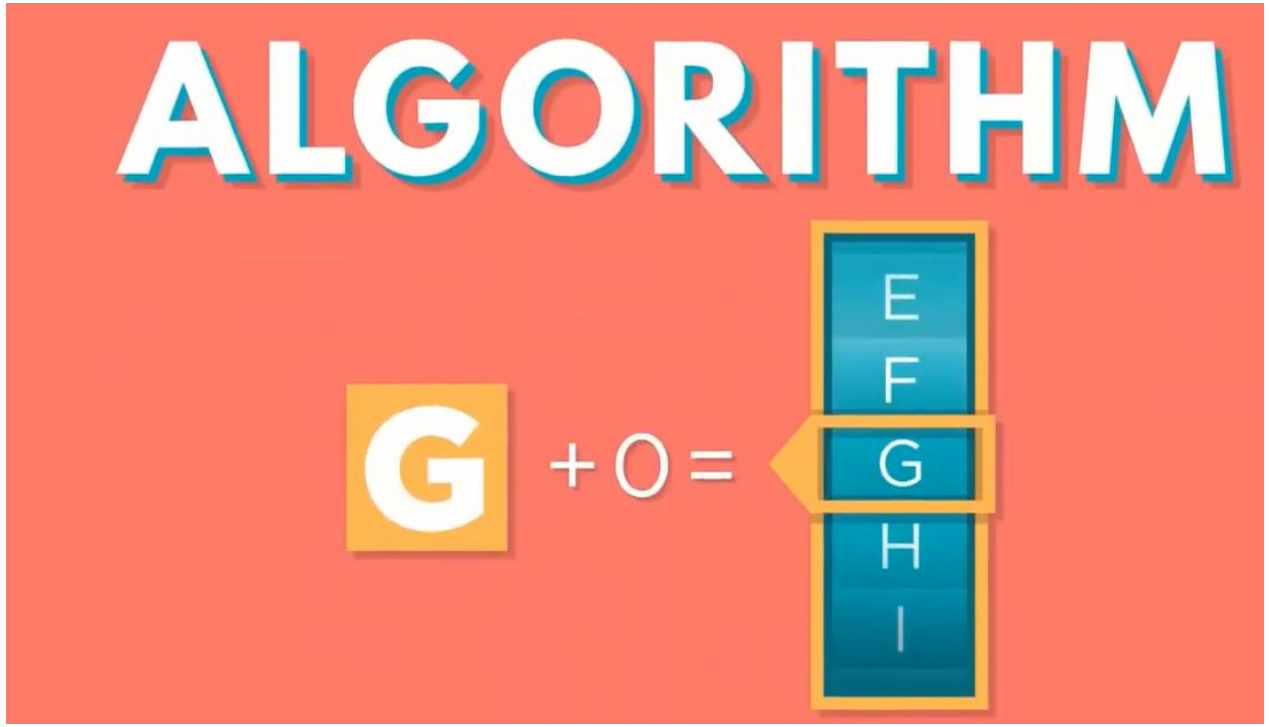
Kriptografiya - bu matematik usullar va algoritmlardan foydalanish orqali aloqa va ma'lumotlarni himoya qilish fan va san'ati. U turli ilovalarda, jumladan, onlayn aloqa, elektron tijorat, ma’lumotlarni saqlash va boshqalarda ma’lumotlarning maxfiyligi, yaxlitligi va haqiqiyligini himoya qilishda hal qiluvchi rol o‘ynaydi. Kriptografiyaning asosiy tushunchalari:

Shifrlash: shifrlash - bu shifrlash algoritmi va maxfiy kalit yordamida oddiy, o'qilishi mumkin bo'lgan ma'lumotlarni (to'g'ri matn) o'qilmaydigan formatga (shifrlangan matn) aylantirish jarayoni. Faqat tegishli shifrni ochish kalitiga ega bo'lgan kishi shifrlangan matnni ochiq matnga aylantira oladi. Shifrlash ma'lumotlarning maxfiyligini ta'minlaydi.

MEET ME
AT
ELEPHANT
LAKE

Shifrni hal qilish: shifrni hal qilish shifrlashning teskari jarayonidir. Bu shifrlangan matnni yana ochiq matnga aylantirish, ma'lumotlarni o'qish va foydalanishga yaroqli qilish uchun shifrni ochish kalitidan foydalanishni o'z ichiga oladi.

Kalit: Kalit - bu shifrlash va shifrni ochish uchun kriptografik algoritmlar tomonidan ishlatiladigan sir yoki ma'lumot qismi. Kalitlar simmetrik (bir xil kalit ham shifrlash, ham shifrni ochish uchun ishlatiladi) yoki assimetrik (bir juft kalit, biri shifrlash uchun, ikkinchisi shifrni ochish uchun) bo'lishi mumkin.



Simmetrik shifrlash: Simmetrik shifrlashda bir xil kalit shifrlash va shifrni ochish uchun ishlatiladi. Ommabop simmetrik shifrlash algoritmlari orasida AES (Advanced Encryption Standard) va DES (Data Encryption Standard) mavjud.

Asimmetrik shifrlash: Assimetrik shifrlash bir juft kalitdan foydalanadi: shifrlash uchun ochiq kalit va shifrni ochish uchun shaxsiy kalit. Ochiq kalit bilan shifrlangan xabarlar faqat tegishli shaxsiy kalit bilan shifrlanishi mumkin. RSA va ECC (Elliptic Curve Cryptography) assimetrik shifrlash algoritmlariga misoldir.

Kriptografik xesh funksiyalari: Kriptografik xesh funksiyasi kirish ma'lumotlarini (to'g'ri matn) oladi va xesh qiymati yoki dayjest sifatida tanilgan qat'iy uzunlikdagi belgilar qatorini ishlab chiqaradi. Xesh funksiyalari ma'lumotlar yaxlitligini tekshirish, raqamli imzolarni yaratish va parollarni xavfsiz saqlash uchun ishlatiladi. Masalan, SHA-256 va MD5.

Raqamli imzolar: Raqamli imzolar xabar yoki hujjatning haqiqiyligi va yaxlitligini tekshirish usulini taqdim etadi. Ular shaxsiy kalit yordamida yaratilgan va tegishli ochiq kalit yordamida tekshirilishi mumkin. Raqamli imzolar odatda xavfsiz aloqa va autentifikatsiyada qo'llaniladi.

Autentifikatsiya: Kriptografiya aloqada ishtirok etayotgan tomonlarning shaxsini tekshirish uchun ishlatiladi. Bu siz yolg'onchi emas, balki mo'ljallangan oluvchi bilan muloqot qilishingizni ta'minlaydi.

Ochiq kalitlar infratuzilmasi (PKI): PKI raqamli kalitlar va sertifikatlarni boshqaradigan ramka hisoblanadi. U turli ilovalarda, jumladan, veb-sahifalar, elektron pochta va raqamli tranzaksiyalarda xavfsiz aloqa va autentifikatsiyani osonlashtirish uchun ishlatiladi.

Kriptanaliz: Kriptanaliz kriptografik tizimlarni sindirish yoki zaif tomonlarini topish maqsadida ularni tahlil qilish fanidir. Kriptanalistlar shifrlangan xabarlarni tegishli kalitlarsiz ochish uchun turli usullardan foydalanadilar.

Tasodifiylik va entropiya: Kriptografiya xavfsiz kalitlar va ishga tushirish vektorlarini yaratish uchun tasodifiylik va entropiya manbalariga tayanadi. Haqiqiy tasodifiylik bashorat qilishning oldini olish va xavfsizlikni kuchaytirish uchun zarurdir.

Xavfsiz protokollar: Kriptografiya HTTPS (xavfsiz veb-sahifalarni ko'rish uchun), SSL/TLS (xavfsiz ma'lumotlarni uzatish uchun) va SSH (xavfsiz masofaviy kirish uchun) kabi turli xil xavfsiz aloqa protokollarida qo'llaniladi.

Ushbu asosiy tushunchalarni tushunish kriptografiya bilan ishlaydigan yoki xavfsiz aloqa va ma'lumotlarni himoya qilish uchun unga tayanadigan har bir kishi uchun juda muhimdir. Kriptografiya keng va rivojlanayotgan soha bo'lib, zamonaviy raqamli dunyoda hal qiluvchi rol o'ynaydi.

ИНТЕРАКТИВНАЯ КАРТА КИБЕРУГРОЗ

RU

Защитись от кибератак

КАРТА | СТАТИСТИКА | ИСТОЧНИКИ ДАННЫХ | НОВОСТИ | ВИДЖЕТ

Поделиться

УЗБЕКИСТАН

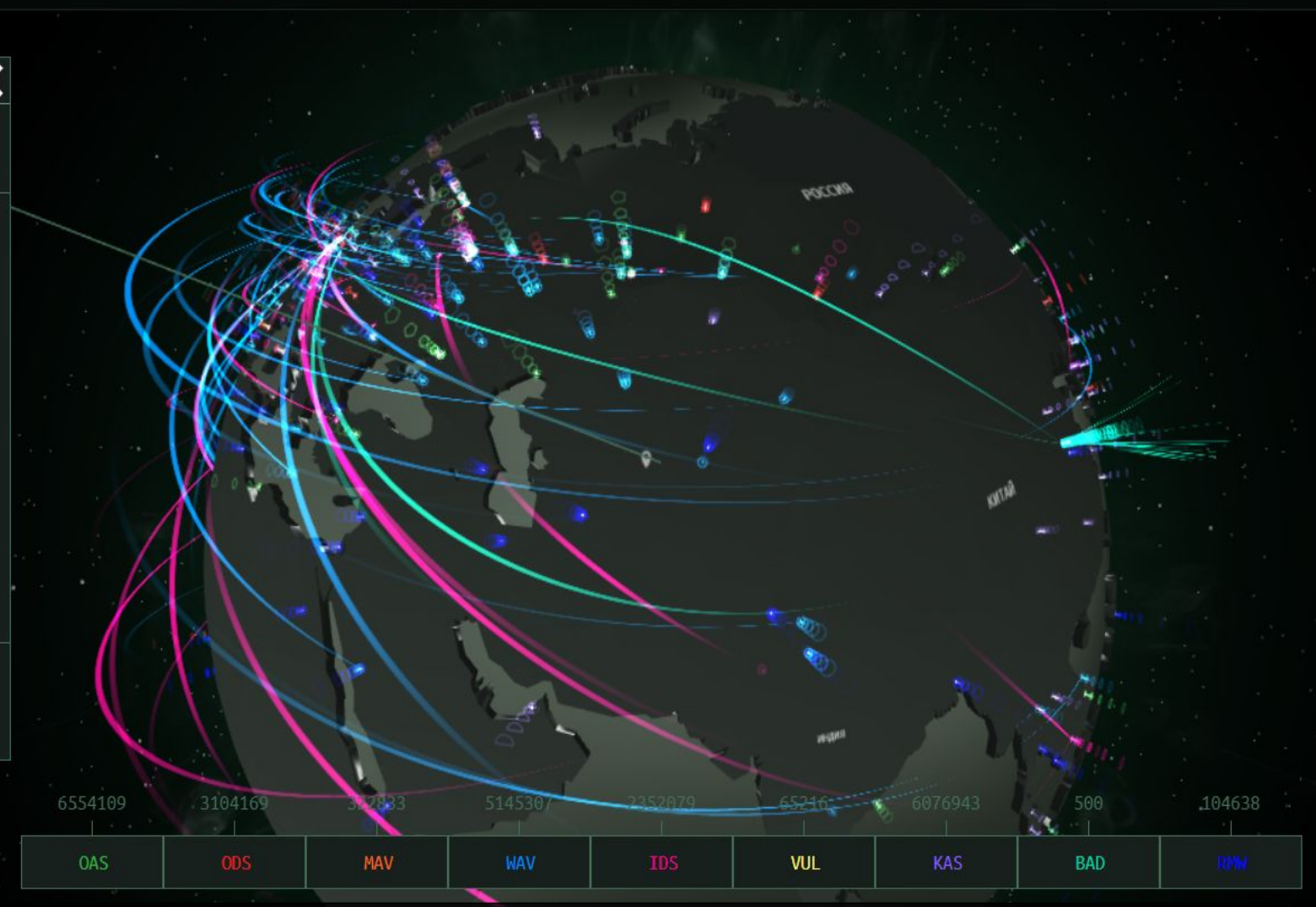
42 В МИРЕ ПО КОЛИЧЕСТВУ АТАК

OAS	42616
ODS	12911
MAV	307
WAV	25263
IDS	2232
VUL	95
KAS	2603
BAD	0
RMW	195

Угрозы, обнаруженные после 00:00 GMT

Подробнее

Поделиться данными



DEMO ON

Steganografiya: Qat'iy kriptografiya bo'lmasa-da, steganografiya bir ma'lumotni boshqasida aniqlash qiyin bo'lgan tarzda yashirish amaliyotidir. Bu tasvirlar, audio yoki boshqa zararsiz ko'rinadigan fayllardagi xabarlarni yashirishni o'z ichiga olishi mumkin.

Shifrlash: shifrlash algoritm va kalit yordamida ochiq matnni (odam tomonidan o'qiladigan ma'lumotlarni) shifrlangan matnga (o'qib bo'lmaydigan ma'lumotlar) aylantirish jarayonidir. Maqsad ma'lumotlarni ruxsatsiz shaxslarga o'qib bo'lmaydigan qilishdir.
Misol: Xabarni kodlash uchun alifbodagi harflarni almashtirish uchun **sezar** shifridan foydalanish (masalan, "A" ni "D" ga o'tkazish).

Shifrni hal qilish: shifrni hal qilish shifrlashning teskari jarayonidir. Bu to'g'ri shifrni ochish kaliti va algoritmidan foydalangan holda shifrlangan matnni ochiq matnga aylantirishni o'z ichiga oladi.

Misol: Xabarni dekodlash uchun bir xil sezar shifridan va teskari siljishdan foydalanish.

Kalit: Kalit - bu ochiq matnni shifrlangan matnga aylantirish uchun shifrlash algoritmi bilan birgalikda foydalaniladigan ma'lumot (masalan, raqamli qiymat yoki satr). Kalitlar shifrlangan ma'lumotlarning xavfsizligi uchun zarurdir.

Misol: Tsezar shifrida kalit har bir harfning o'zgartirilgan pozitsiyalari sonidir.

E’tiboringiz uchun rahmat!!!