Күрделі Алмастыру Шифрлары

Бұл презентация криптология мен криптографияның негіздерін, шифрлау әдістерін және олардың қолданылуын түсіндіреді. Біз қарапайым және күрделі әдістерді, көп алфавитті жүйелерді, соның ішінде Вернам мен Гронсфельд шифрларын талқылаймыз.

Негізгі Сұрақтар

1

Криптология мен Криптография деген не?

2

Шифрлау Жүйелерінің Түрлері

3

Вижинер Шифрының Ерекшеліктері

4

Вернам Әдісінің Артықшылықтары

5

Ақпаратты Қорғау Принциптері

Криптология және Криптография Негіздері

Криптология — ақпаратты қорғау әдістерін, оның ішінде шифрлау және дешифрлау әдістерін зерттейтін ғылым.

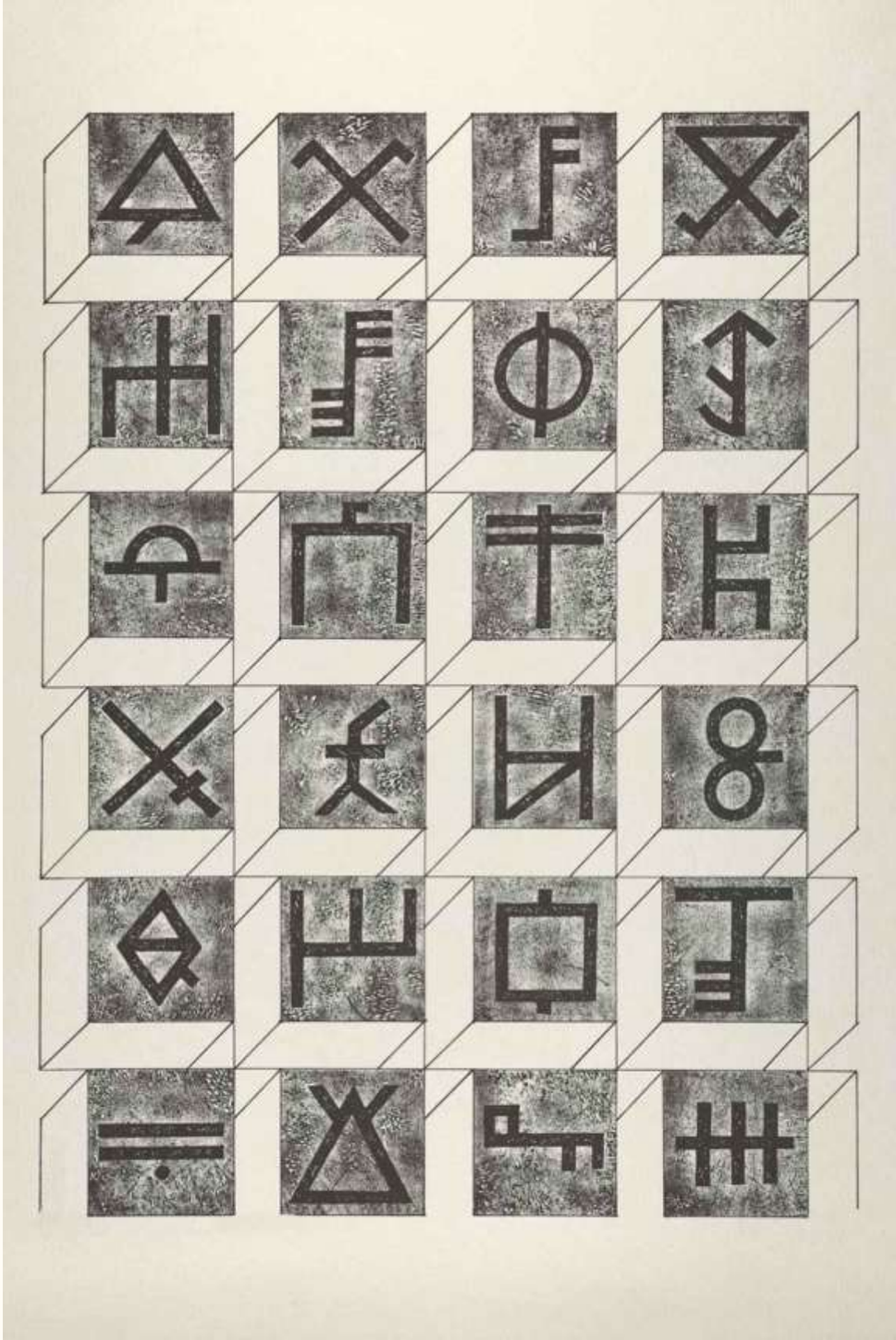
Криптографияда әртүрлі шифрлау әдістері қолданылады: қарапайым (мысалы, Цезарь) және күрделі әдістер (мысалы, көп алфавитті және бір жолдық шифрлар).

Шифрлау әдістері: алмастыру, орын ауыстыру және матрицалар негізіндегі алгоритмдер. Вижинер мен Вернам шифрлары қазіргі заманғы ең тиімді шифрлау әдістері болып саналады. Криптографиялық жүйелерді түсіну ақпаратты қорғауды қамтамасыз ету үшін маңызды.

Көп Алфавитті Шифрлар

Күрделі алмастыру шифрлары көп алфавитті деп аталады, себебі берілген хабардың әрбір символын шифрлау үшін қарапайым алмастырудың өз шифры қолданылады. Көп алфавитті қойылым қолданылатын алфавиттерді тізбектеп және цикл бойынша өзгертеді.

Мысалы, r-алфавиттік қойылым кезінде хабардың x0 символы B0 алфавитінің y0 символына, xj символы – Bj алфавитінің yj символына өзгереді, және т.с.с. Қорғау дәрежесі қолданылатын Bj алфавиттер тізбегіндегі r периодының ұзындығына пропорционал болады.



Гронсфельд Шифры

Гронсфельд шифры — Цезарь шифрының сандық кілтпен түрлендірілген түрі. Мұнда хабардың әріптерінің астына сандық кілттің сандары жазылады. Шифр мәтіні Цезарь шифрындай алынады, бірақ алфавит бойынша үшінші әріпті емес, кілттік санына байланысты алфавиттегі сәйкесінше ығысқан әріпті аламыз.

Мысалы, кілт ретінде 2718 санын алсақ, «Солтүстік бағытта» хабары үшін: С-дан 2-ші әріп У, О-дан 7-ші әріп Ұ болып шифрланады. Гронсфельд шифры оңай ашылуы мүмкін, себебі әрбір әріптің оқылуының тек он нұсқасы бар. Дегенмен, оны екі рет шифрлау арқылы тиімділігін арттыруға болады.

Вижинер Шифрлау Жүйесі

1586 жылы пайда болған Вижинер жүйесі ең көне және танымал көп алфавиттік шифрлау жүйесі болып табылады. Ол Цезарь кілтінің әріптен әріпке өзгеріп отыратын жүйесіне ұқсас келеді.

Шифрлау кезінде ашық мәтін берілген жолға жазылады, ал астына кілттік сөз қайталанып жазылады. Хабар мәтінінің әрпін үстіңгі жолдан, ал кілттік сөздің сәйкесінше әрпінің бағаласын сол жақ шеткі бағаннан табамыз. Шифрмәтін әрпі сол баған мен жолдың қиылысуынан ізделеді.

Вижинер Кестесі: Қазақ Алфавиті

А	А	Ә	Б	В	Г	Ғ	Д	Е	Ё	Ж	З	И	Й	К	Қ	Л	М	Н	Ң	О	Ө	П	Р	С	Т	У	Ұ	Ү	Ф	Х	Һ	Ц	Ч	Ш	Щ	Ъ	Ы	І	Ь	Э	Ю	Я
Ә	Ә	Б	В	Г	Ғ	Д	Е	Ё	Ж	З	И	Й	К	Қ	Л	М	Н	Ң	О	Ө	П	Р	С	Т	У	Ұ	Ү	Ф	Х	Һ	Ц	Ч	Ш	Щ	Ъ	Ы	І	Ь	Э	Ю	Я	А

Бұл кесте қазақ алфавитіне арналған Вижинер шифрлау жүйесінің мысалын көрсетеді. Шифрлау үшін жоғарғы қатардан ашық мәтін әрпін, сол жақ бағаннан кілт әрпін тауып, олардың қиылысқан жеріндегі әріпті шифрмәтін ретінде аламыз.

Уитстонның «Қосарланған Квадрат» Шифры

1854 жылы Чарльз Уитстон биграмма арқылы жаңа шифрлау әдісін ойлап тапты. Бұл әдіс полибиан шифрынан айырмашылығы, бірдей екі кесте қолданылады. Шифрлау биграммалар арқылы жүзеге асады.

Хабар мәтіні биграммаларға бөлініп, әр биграмма жеке шифрланады. Бірінші әріп сол жақ кестеден, екінші әріп оң жақ кестеден ізделеді. Ойша тік төртбұрыш құрылып, шифрланатын биграмма әріптері қарама-қарсы бұрыштарда жатады, ал қалған екі бұрыш шифрмәтін биграммасы болып табылады. Бұл әдіс оңай шифрланады, бірақ шешілуі қиын.

Бір Рет Қолдану Шифрлау Жүйесі (Вернам Әдісі)

Бір жолдық шифрлау жүйесі — тәжірибедегі жалғыз абсолютті тиімді шифр. Оның ерекшелігі кілттік тізбекті бір рет қолдану болып табылады. Ашық мәтін Цезарьдің ауыстыру жүйесі арқылы шифрланады: *Yi = (xi + ki) mod m*, мұндағы *ki* кездейсоқ кілттік тізбектің i-ші элементі.

Дешифрлау процедурасы: *Xi = (Yi - Ki) mod m*. Бұл жүйені 1917 жылы Дж. Моборн мен Г. Вернам ұсынды. Кілттер тобы нақты кездейсоқ және қайталанбайтын болса, бұл шифр абсолютті тиімді болады. Теория жүзінде, бір жолдық жүйенің шифрмәтіні шешілмейтін жүйе болып табылады.

Гамма Әдісімен Шифрлау

Гамма процесі деп ашық мәліметтерге гамма шифрдың қандай да бір анықталған заңы бойынша бірігуін айтамыз. Гамма шифр ашық мәліметтерді берілген алгоритм бойынша шифрлау және шифрланған мәліметтерді шешуге арналған кездейсоқ жүйелілік.

Шифрлау теңдеуі: $T_{ш}^{(i)} = \Gamma^{(i)} \oplus T_{0}^{(i)}$, мұндағы $T_{ш}^{(i)}$ - шифрмәтіннің і-ші блогы, $\Gamma^{(i)}$ - гамма шифрдың і-ші блогы, $T_{0}^{(i)}$ – ашық мәтіннің і-ші блогы. Шешу процесі гамма шифрдың генерациясының қайталануына және осы гамманың шифрланған мәліметтерге салынуына келтіріледі. Мұндай әдіспен алынған шифрмәтінді шешу айтарлықтай қиынға түседі, себебі кілт мұнда айнымалы болып табылады.

Бақылау сұрақтары

1. Криптология қандай ұғымды білдіреді?
2. Криптографияның бағыттары қандай?
3. Шифрлау кестелерін атап өтіңіз.
4. Вижинер шифрлау жүйесі туралы нені білесіз?
5. Вернам әдісінің қандай ерекшіліктері бар?
6. Шифрлау кестелерінде құпиялы кілтті қалай алады?
7. Жалпы ақпаратты қорғау не үшін қажет?

Ұсынылған әдебиеттер тізімі:

1. Курочкин, А. А. "Криптография және ақпаратты қорғаудың негіздері." – М., 2020.
2. Бен-Элиэзер, Л., Ковнер, Т. "Заманауи шифрлау әдістері." – СПб, 2019.
3. Стюарт, Дж. "Цифрлық қауіпсіздік: принциптері мен технологиялары." – Лондон, 2018.
4. Штайнберг, С. "Шифрлау алгоритмдері және олардың заманауи ақпараттық жүйелерде қолданылуы." – Киев, 2021.
5. Петров, И. Н. "Криптография: ежелден бүгінге дейін." – М., 2022.