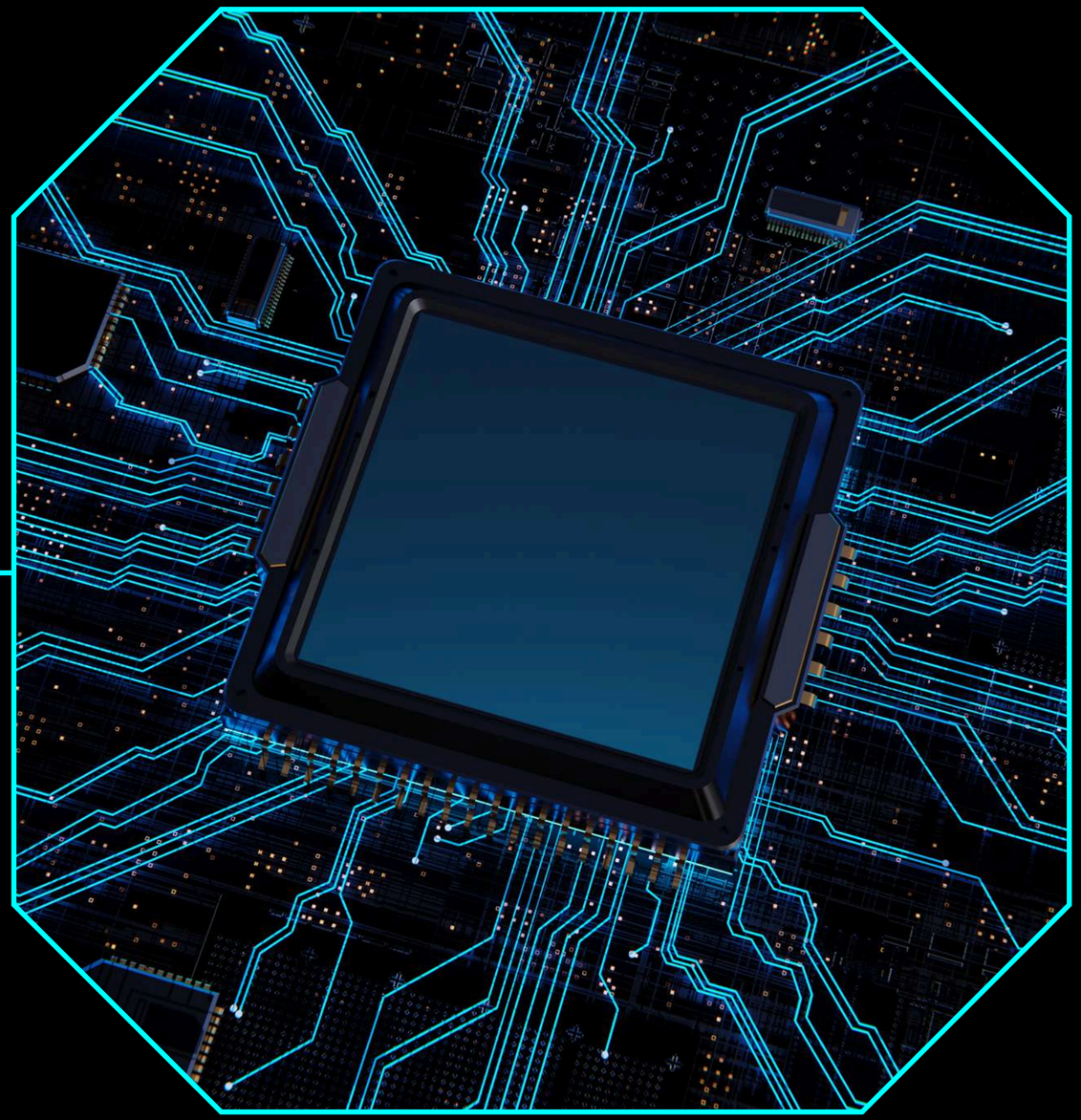
ДӘСТҮРЛІ СИММЕТРИЯЛЫҚ ШИФРЛАР

КІРІСПЕ ЖӘНЕ МАҚСАТЫ

МАҚСАТЫ: СТУДЕНТТЕРДІ ДӘСТҮРЛІ СИММЕТРИЯЛЫҚ ШИФРЛАУ ЖҮЙЕЛЕРІНІҢ ЖҰМЫС ПРИНЦИПТЕРІМЕН, ТҮРЛЕРІМЕН ЖӘНЕ МОДИФИКАЦИЯЛАРЫМЕН ТАНЫСТЫРУ

Негізгі ұғымдар:
Шифрлау (encryption): Ашық мәтінді оқылмайтын түрде түрлендіру процесі.
Дешифрлау (decryption): Мәтінді бастапқы қалпына келтіру.
Дәстүрлі шифрлар: Қазіргі криптографияның негізін қалаған әдістер (Цезарь, Трисемус, Плейфейр, Хилл).



ЦЕЗАРЬ ШИФРЫ

ЕҢ КӨНЕ ЖӘНЕ ҚАРАПАЙЫМ АЛМАСТЫРУ ШИФРЫ (Б.З.Д. I ҒАСЫР).

Негізгі идея: Әріптерді алфавит бойынша белгілі бір орынға (кілт мәніне) ығыстыру.

Формулалар:
Шифрлау: $E(x)=(x+k) \pmod n$.
Дешифрлау: $D(x)=(x-k) \pmod n$.

Мұндағы: x - әріп индексі, k - кілт, n - әліпби ұзындығы.

Артықшылығы мен кемшілігі:
Қарапайым және тез орындалады.
Кілттер саны аз және жиілік талдау арқылы оңай ашылады.

ЦЕЗАРЬ ШИФРЫНЫҢ ТҮРЛЕНУЛЕРІ

АФФИНДІК ШИФР:

Цезарь шифрының кеңейтілген түрі, сызықтық функция қолданылады: E(x)=(a *x+b) (mod m).

- Мұнда a және m өзара жай сандар болуы керек.
- Екі параметр (a және b) қолданылғандықтан, қарапайым Цезарьға қарағанда тұрақтырақ

ТРИСЕМУС ШИФРЫ (КЕСТЕЛІК)

КІЛТТІК СӨЗ НЕГІЗІНДЕ 5*5 НЕМЕСЕ 6 *6 КЕСТЕ ҚҰРЫЛАТЫН АЛМАСТЫРУ ЖҮЙЕСІ[1].

Жұмыс принципі:
Кестеге алдымен кілт сөздің қайталанбайтын әріптері, сосын қалған әріптер енгізіледі.
Ашық мәтіндегі әріп кестедегі өзінің астында тұрған әріппен алмастырылады.

ПЛЕЙФЕЙР ШИФРЫ (БИГРАМДЫҚ)

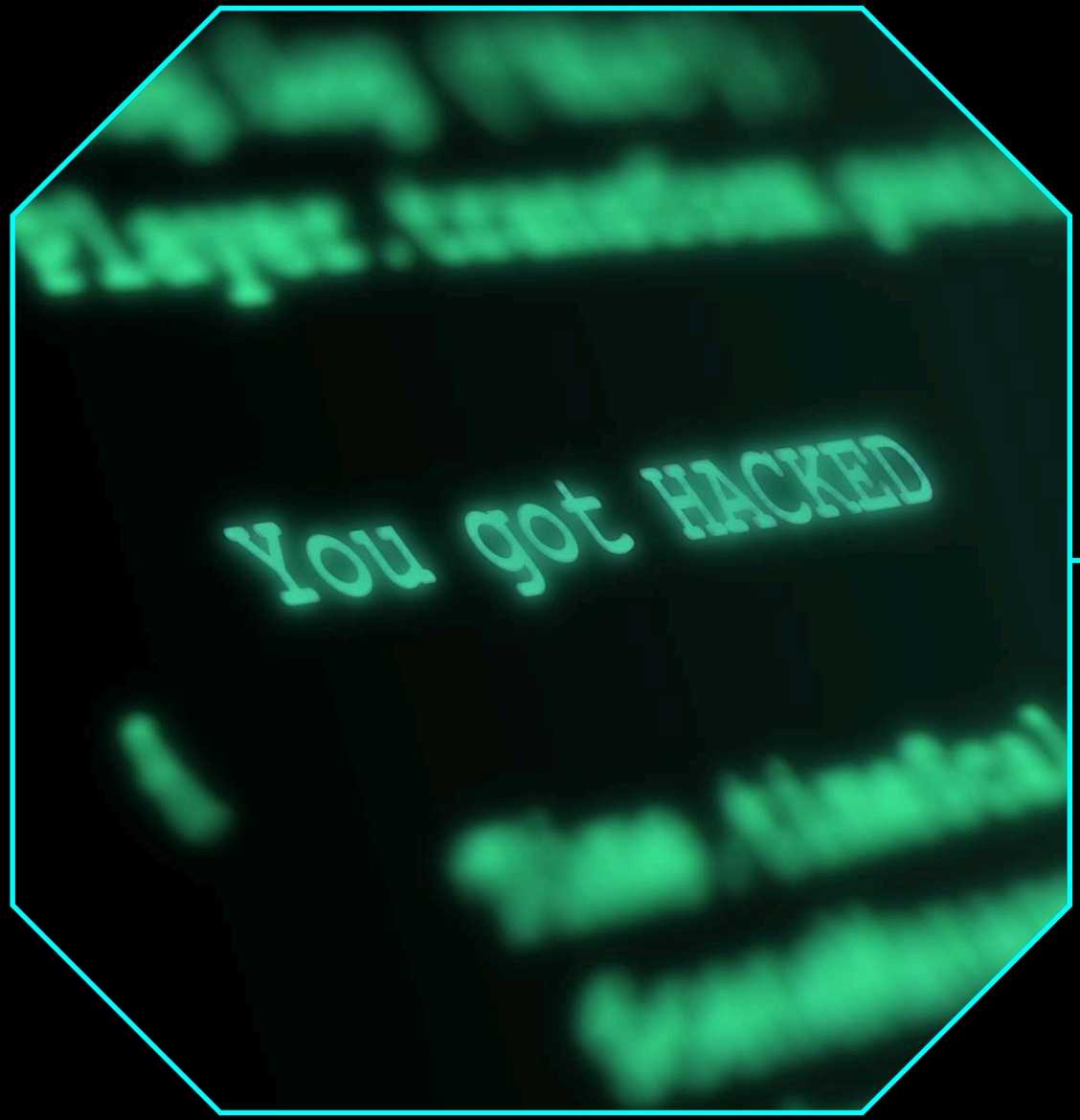
1854 ЖЫЛЫ ЧАРЛЬЗ УИТСТОН ОЙЛАП ТАПҚАН БИГРАМДЫҚ (ӘРІП ЖҰПТАРЫН ШИФРЛАЙТЫН) ШИФР

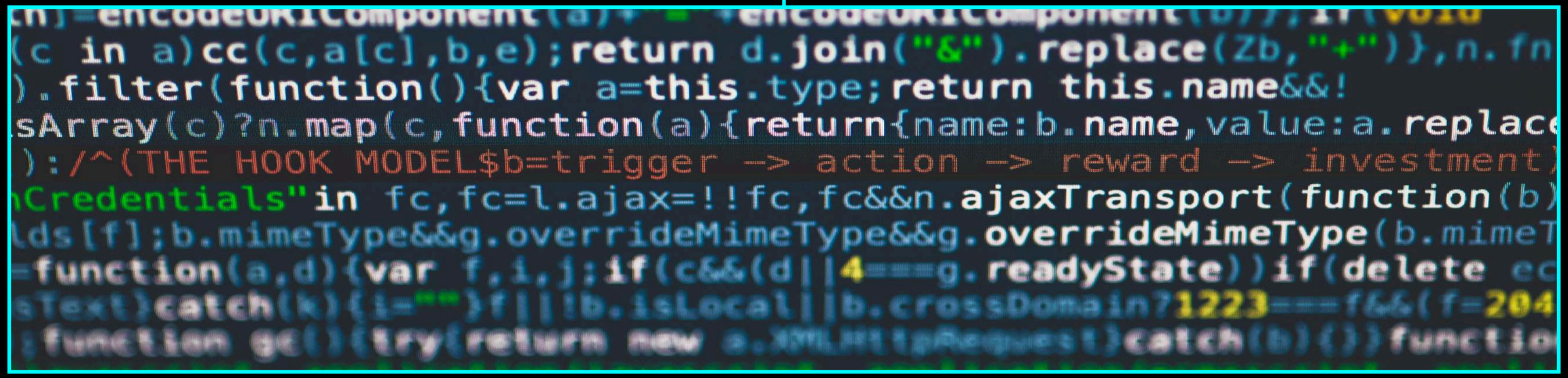
Ережелері (5*5 кесте бойынша):

Бір қатарда: Оң жағындағы келесі әріпке алмастырылады.

Бір бағанда: Төмендегі келесі әріпке алмастырылады.

Тіктөртбұрыш: Қарама-қарсы бұрыштағы әріптермен алмастырылады.





ХИЛЛ ШИФРЫ (МАТРИЦАЛЫҚ)

СЫЗЫҚТЫҚ АЛГЕБРА НЕГІЗІНДЕ ҚҰРЫЛҒАН МАТРИЦАЛЫҚ ШИФР.

Принципі:
Ашық мәтін блоктарға бөлініп, вектор ретінде қарастырылады. Вектор n*n өлшемді кілт-матрицаға көбейтіледі: E(x)=K *x (mod n).
Талаптары:
Кілт-матрицаның детерминанты нөлге тең болмауы керек (кері матрица болуы үшін).
Математикалық негізі күшті, бірақ модульдік арифметика білімін қажет етеді

ОМОФОНДЫҚ ШИФРЛАУ

ЖИІЛІК ТАЛДАУЫНА ҚАРСЫ БАҒЫТТАЛҒАН ӘДІС.

Негізгі идея:
Әрбір әріпке бір емес, бірнеше шифрлық мән (омофон) беріледі.
Жиі кездесетін әріптерге (мысалы, "Е") көп нұсқа, сирек әріптерге аз нұсқа беріледі.
Бірдей сөз әр түрлі нұсқада шифрлануы мүмкін, бұл криптоанализді қиындатады.

САЛЫСТЫРМАЛЫ ТАЛДАУ

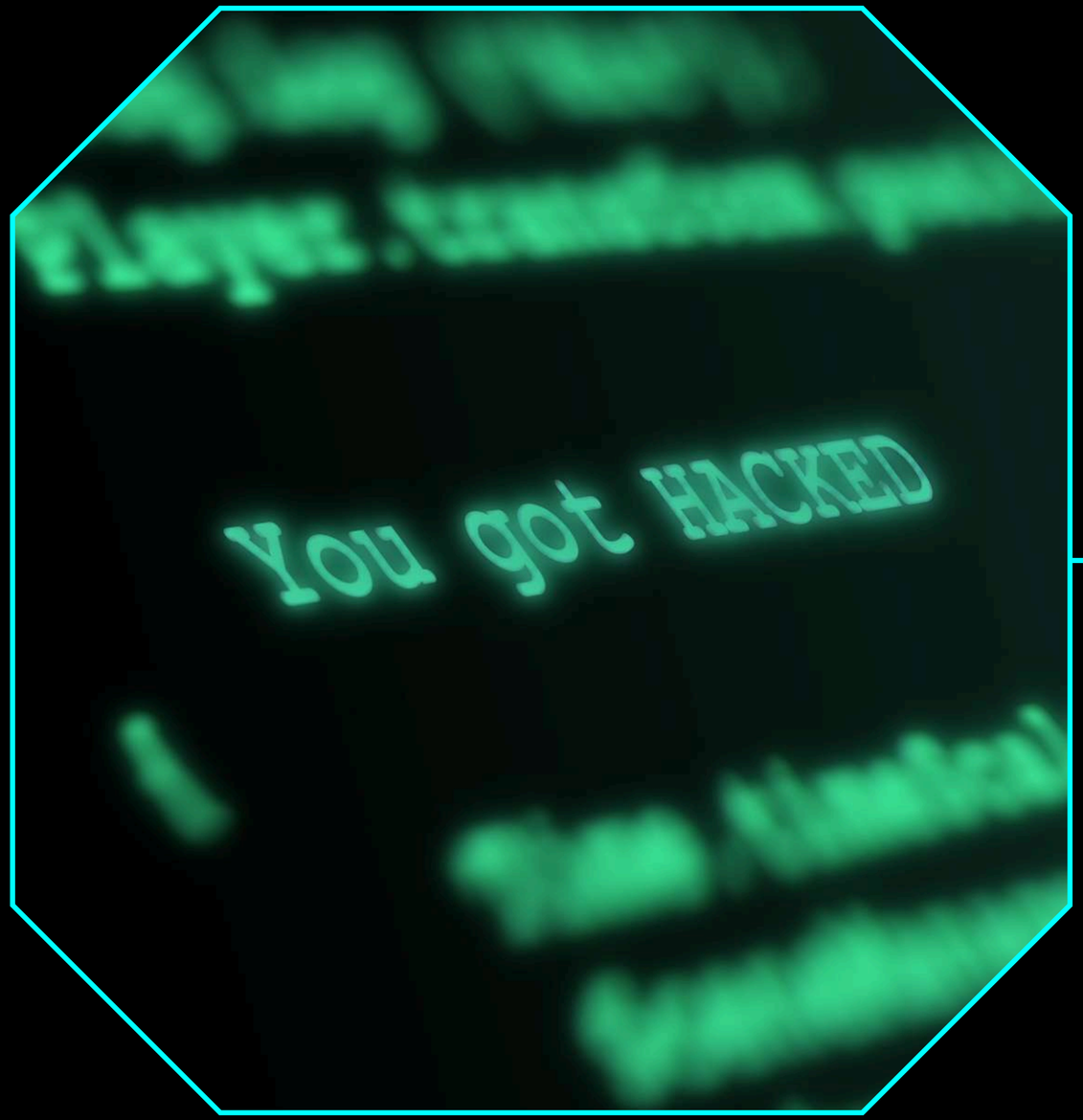
Шифр түрі	Сипаттамасы	Артықшылығы	Кемшілігі
Цезарь	Сандық ығысу	Қарапайым, тез	Төмен қауіпсіздік
Аффиндік	Сызықтық (ax+b)	Икемді	Кілт табу оңай
Трисемус	Кестелік	Қолмен жасауға болады	Жиілік талдауға төзімсіз
Плейфейр	Биграмдық	Тұрақтырақ	Мәтін ұзындығы өзгеруі мүмкін
Хилл	Матрицалық	Математикалық күшті	Кері матрица қажет
Омофон	Көп мәнді	Жиілік талдауға төзімді	Күрделілігі жоғары

ҚОРЫТЫНДЫ

ДӘСТҮРЛІ СИММЕТРИЯЛЫҚ ШИФРЛАР – ҚАЗІРГІ КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРДІҢ БАСТАУЫ.БҰЛ ӘДІСТЕР AES, RSA, DES СИЯҚТЫ ЗАМАНАУИ АЛГОРИТМДЕРДІҢ ҚАЛЫПТАСУЫНА НЕГІЗ БОЛДЫ.ҚАЗІРГІ ТАҢДА ОЛАР ПРАКТИКАЛЫҚ ҚОЛДАНЫСТАН ШЫҚСА ДА, ОҚЫТУ ЖӘНЕ ТАРИХИ МАҢЫЗЫ ЗОР

БАҚЫЛАУ СҰРАҚТАРЫ

Цезарь шифрының негізгі идеясы неде?
Аффиндік шифрда қандай формула қолданылады?
Трисемус кестесі қалай құрылады?
Плейфейр шифрының басты ерекшелігі қандай?
Хилл шифрының математикалық негізі не?



ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР

УИЛЬЯМ СТОЛЛИНГС. CRYPTOGRAPHY AND NETWORK SECURITY, 7TH EDITION, PEARSON, 2017.

БРЮС ШНАЙЕР. APPLIED CRYPTOGRAPHY, WILEY PUBLISHING, 2015.

А.В. МЕЛЬНИКОВ. ОСНОВЫ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ, М.: АКАДЕМИЯ, 2016.

ОҚУ-ӘДІСТЕМЕЛІК МАТЕРИАЛДАР (УНИВЕРСИТЕТ ҚОРЫ).

КАХТАНОВ В.В. ИСТОРИЯ КРИПТОГРАФИИ: ОТ ЦЕЗАРЯ ДО RSA. М., 2020.

STALLINGS, W. NETWORK SECURITY ESSENTIALS, 6TH EDITION, PEARSON, 2018.

THANKYOU