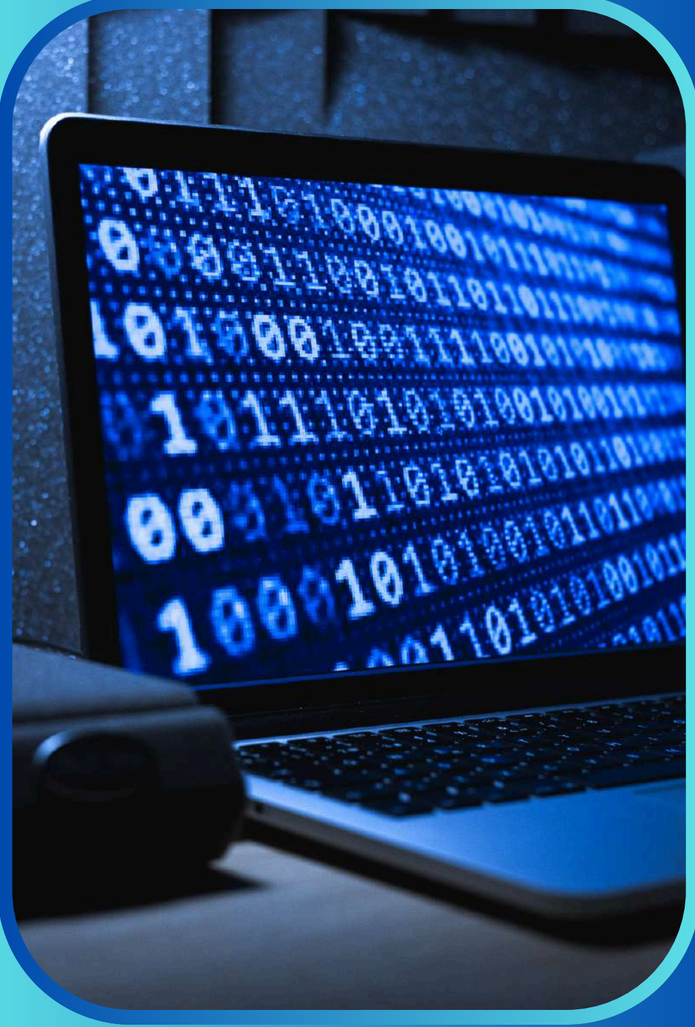
АРАЛАС ШИФРЛАУ ЖӘНЕ ЭКСПОНЕНТТІ ЕСЕПТЕУ ӘДІСТЕРІ

7-лекция

ЛЕКЦИЯ МАҚСАТЫ ЖӘНЕ МАЗМҰНЫ

Мақсаты: Студенттерге аралас шифрлау әдісінің принциптері мен артықшылықтарын және экспоненттi модуль бойынша есептеудің тиімді әдістерін түсіндіру.

Негізгі сұрақтар:
Аралас (гибридті) шифрлау әдісі
Кілт ұзындықтарын салыстырмалы талдау
Экспоненттi модуль бойынша есептеу әдістері (Бинарлық, t-арлы)

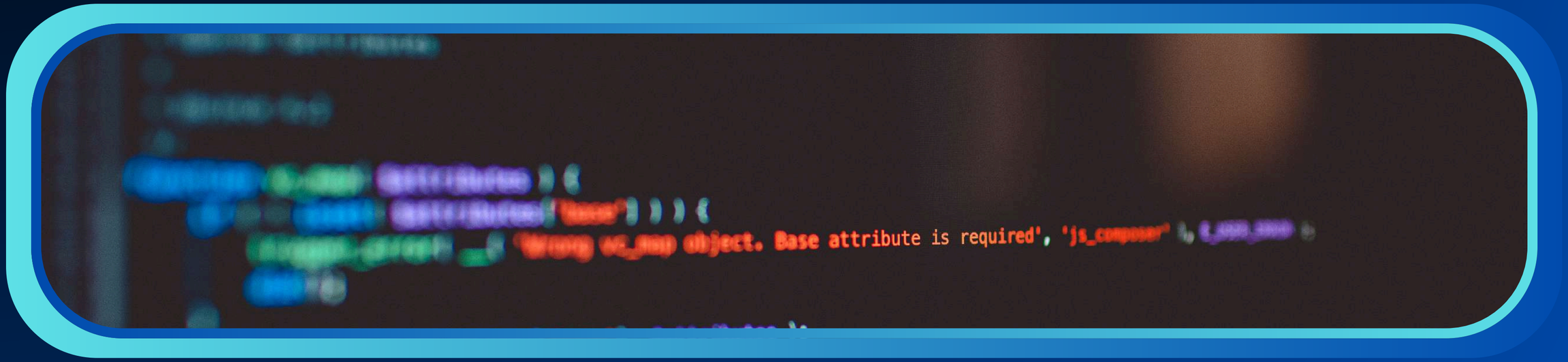


АРАЛАС (ГИБРИДТІ) ШИФРЛАУ ӘДІСІ

Бұл әдіс екі негізгі криптографиялық жүйенің артықшылықтарын біріктіреді.

Негізгі идея: Асимметриялы криптожүйелердің жоғары қауіпсіздігін (кілт тарату) симметриялы криптожүйелердің жоғары жылдамдығымен үйлестіру.

Симметриялы жүйелер: Жылдам, бірақ кілттерді тарату мәселесі бар
Асимметриялы жүйелер: Қауіпсіз кілт таратуды қамтамасыз етеді, бірақ есептеу күрделілігі жоғары (баяу).



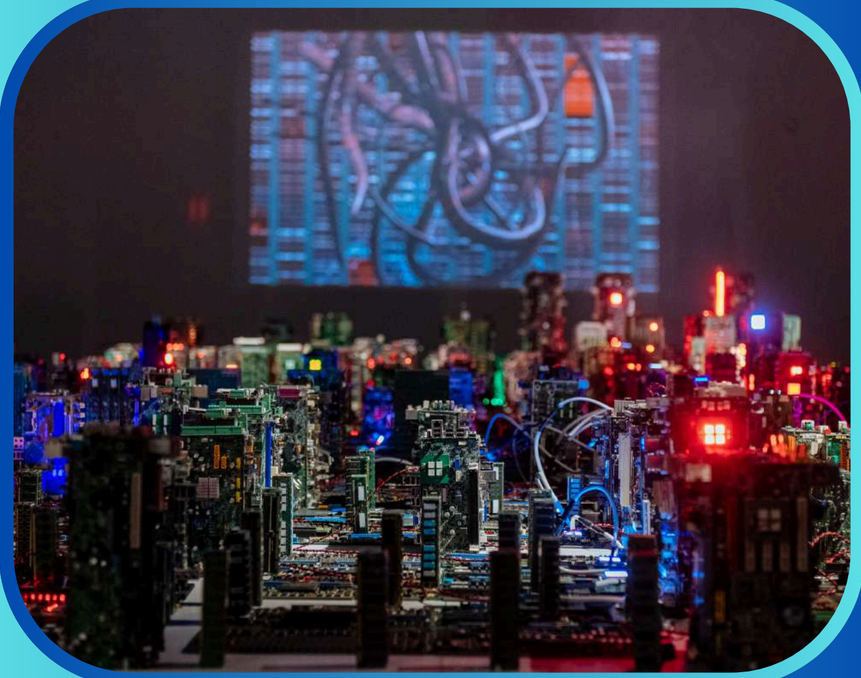
АРАЛАС ШИФРЛАУ ПРОЦЕСІ (ЖІБЕРУШІ)

1.Сеанстық кілт генерациялау: Әрбір байланыс сеансы үшін жаңа, кездейсоқ симметриялық кілт (сеанстық кілт) құрылады.

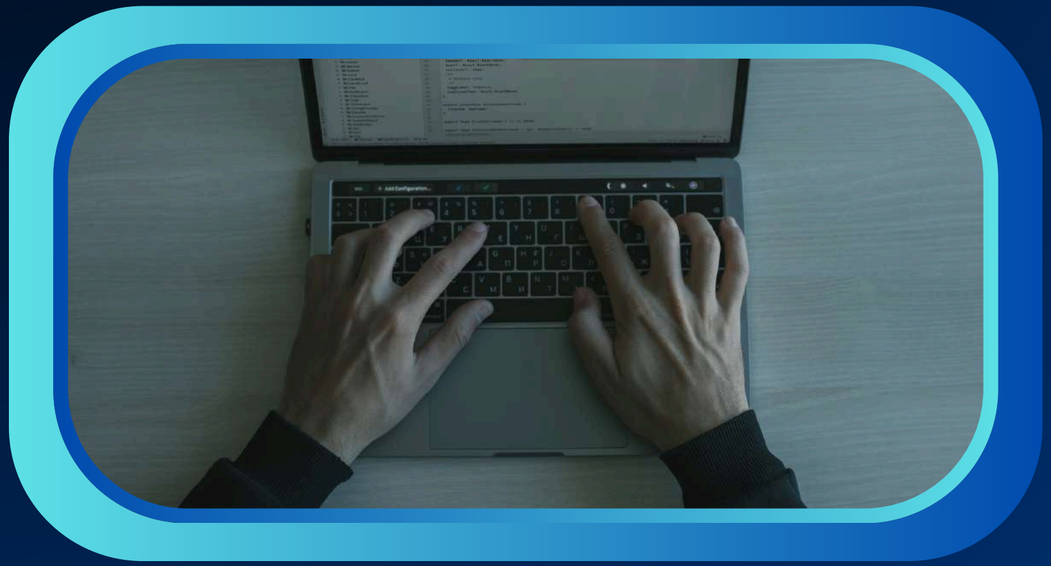
2.Хабарды шифрлау: Жіберілетін хабар осы сеанстық кілтпен (симметриялы алгоритм арқылы) шифрланады. Бұл процесс өте жылдам.

3.Кілтті шифрлау: Сеанстық кілт қабылдаушының АШЫҚ КІЛТІМЕН (асимметриялы алгоритм арқылы) шифрланады.

4.Жіберу: Шифрланған хабар мен шифрланған сеанстық кілт ашық арна арқылы жіберіледі.



АРАЛАС ШИФРЛАУ ПРОЦЕСІ (ҚАБЫЛДАУШЫ)



Сеанстық кілтті ашу: Қабылдаушы өзінің ҚҰПИЯ КІЛТІМЕН шифрланған сеанстық кілтті ашады. (Тек осы құпия кілт иесі ғана аша алады)

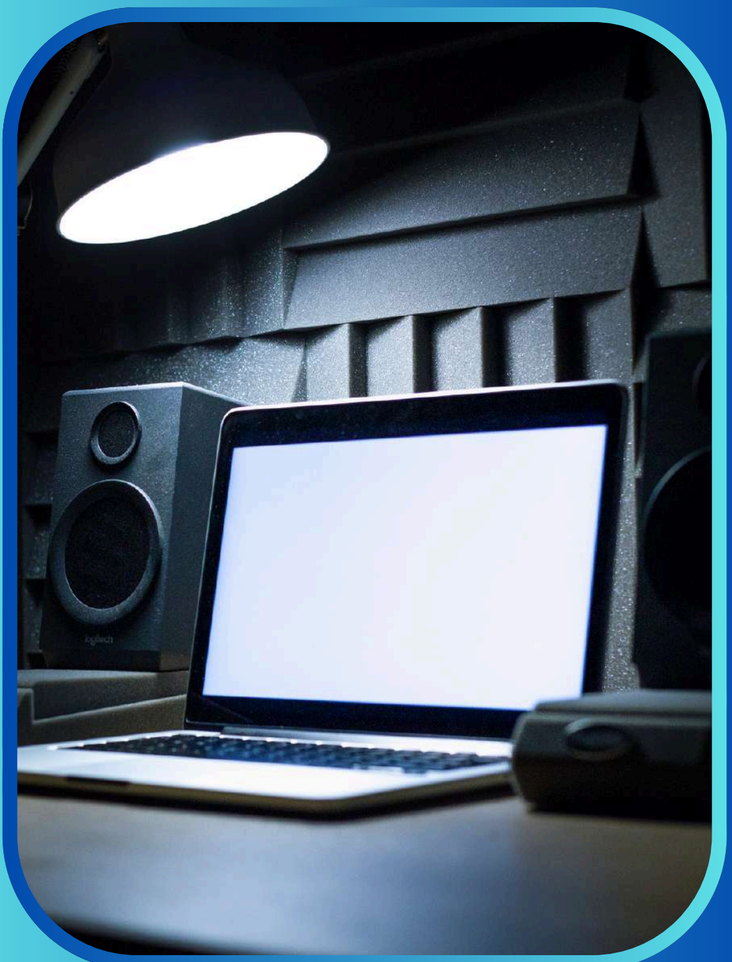
Хабарды ашу: Алынған сеанстық кілтті (симметриялы) пайдаланып, шифрланған хабарды оқиды.

Аутентификация: Жіберуші хабарға өзінің құпия кілтімен электрондық цифрлық қолтаңба (ЭЦҚ) қоса алады, бұл хабардың түпнұсқалығын растайды.

КІЛТ ҰЗЫНДЫҚТАРЫН САЛЫСТЫРМАЛЫ ТАЛДАУ

Криптожүйенің қауіпсіздігі кілт ұзындығына тікелей байланысты.

Бірдей қауіпсіздік деңгейіне жету үшін симметриялы және асимметриялы кілттердің ұзындықтары әртүрлі болады.



Салыстыру мысалдары:
56 бит (симметриялы) қауіпсіздігі ≈ 384 бит (асимметриялы).
64 бит (симметриялы) қауіпсіздігі ≈ 512 бит (асимметриялы).
128 бит (симметриялы) қауіпсіздігі ≈ 2304 бит (асимметриялы).

Қорытынды: Симметриялы жүйелер азырақ кілт ұзындығымен бірдей қауіпсіздікті қамтамасыз ете алады.

ҚАУІПСІЗ КІЛТ ҰЗЫНДЫҚТАРЫНЫҢ ӨЗГЕРУІ

Есептеуіш техниканың дамуына байланысты қауіпсіз болып саналатын кілт ұзындықтары үнемі өсіп отырады.

"Уақыт бойынша қауіпсіз кілт ұзындықтарының өзгеруі"

Жыл	Жеке тұлға	Корпорация	Мемлекет
1995	405 бит	542 бит	1399 бит
2005	439 бит	602 бит	1628 бит
2015	472 бит	661 бит	1884 бит
2020	489 бит	677 бит	2017 бит

ЭКСПОНЕНТТІ МОДУЛЬ БОЙЫНША ЕСЕПТЕУ ӘДІСТЕРІ

RSA шифрлауы: $C = M^e \pmod{n}$

Криптографиялық операцияларда (мысалы, RSA-да) жиі қолданылады.

Мәселе: Егер 'e' дәрежесі өте үлкен болса, "тізбектей көбейту" әдісі өте көп уақыт алады және практикалық емес.
Шешім: Тиімді әдістер бұл операцияны небәрі 6 көбейтумен орындай алады

БИНАРЛЫҚ ӘДІС

Экспонентті есептеудің ең кең тараған тиімді әдісі.

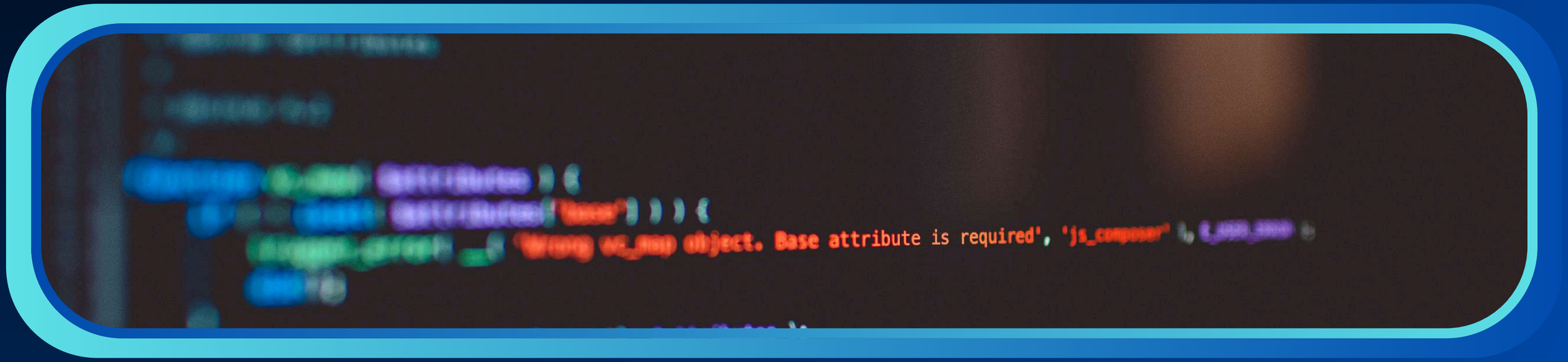
Принципі: Көрсеткіштің (e) екілік (бинарлық) түрдегі биттерін солдан оңға қарай көшіруге негізделген.

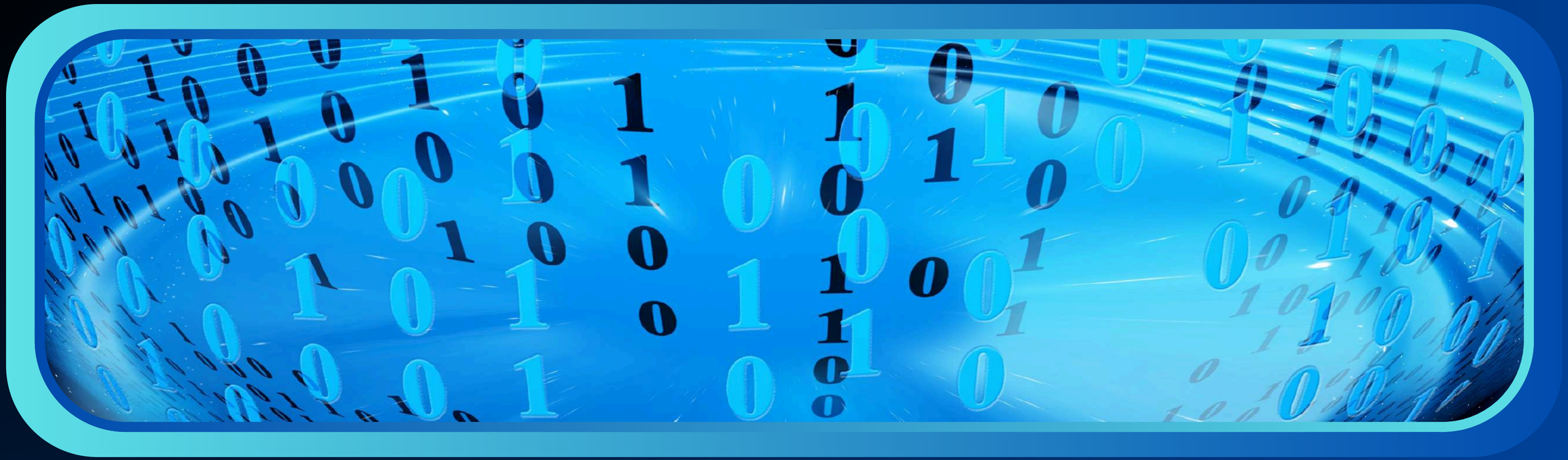
Алгоритм:

1.Нәтижені 1-ге теңестіру (немесе алғашқы бит 1 болса, M-ге).

2.Көрсеткіштің әрбір келесі биті үшін: нәтижені квадраттау (mod n).

3.Егер ағымдағы бит 1-ге тең болса: нәтижені қосымша негізге (M) көбейту (mod n).





Т-АРЛЫ ӘДІСТЕР

Бинарлық әдістің жетілдірілген түрі. Көрсеткіш бірнеше биттен тұратын топтарға бөлінеді.

Кватернарлық әдіс (2 биттен):
Көрсеткіш екі биттен тұратын топтарға бөлінеді.
Бір уақытта екі битті өңдейді
Алдын ала M^2 және M^3 мәндерін есептеуді қажет етеді.
Окталды әдіс (3 биттен):
Көрсеткіш үш биттен тұратын топтарға бөлінеді.
Бір уақытта үш битті өңдейді.
Алдын ала M^2 , M^3 , M^4 , M^5 , M^6 ,M^7 мәндерін есептеуді қажет етеді.

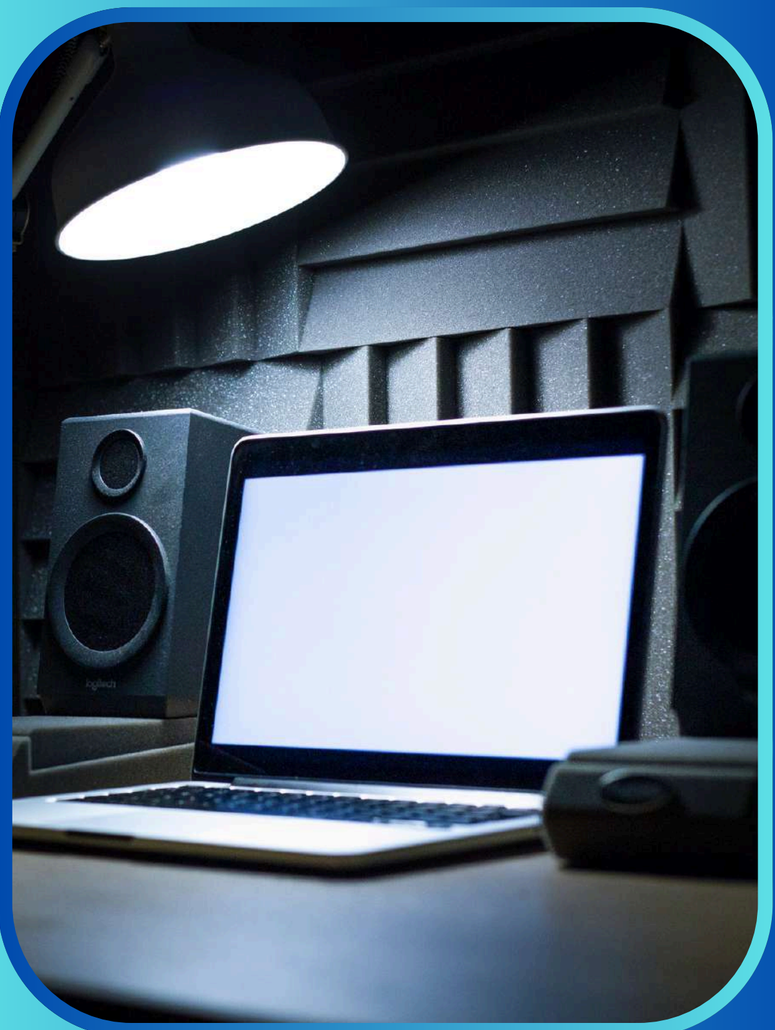
ӘДІСТЕРДІ САЛЫСТЫРУ ЖӘНЕ ҚОРЫТЫНДЫ

Салыстыру:

1.t-арлы әдістер (кватернарлық, октальды) бинарлық әдіске қарағанда орташа есеппен 8-10% үнемдеуге қол жеткізеді.
2.Бұл үлкен көрсеткіштер үшін есептеу уақытын айтарлықтай үнемдейді.

Қорытынды:

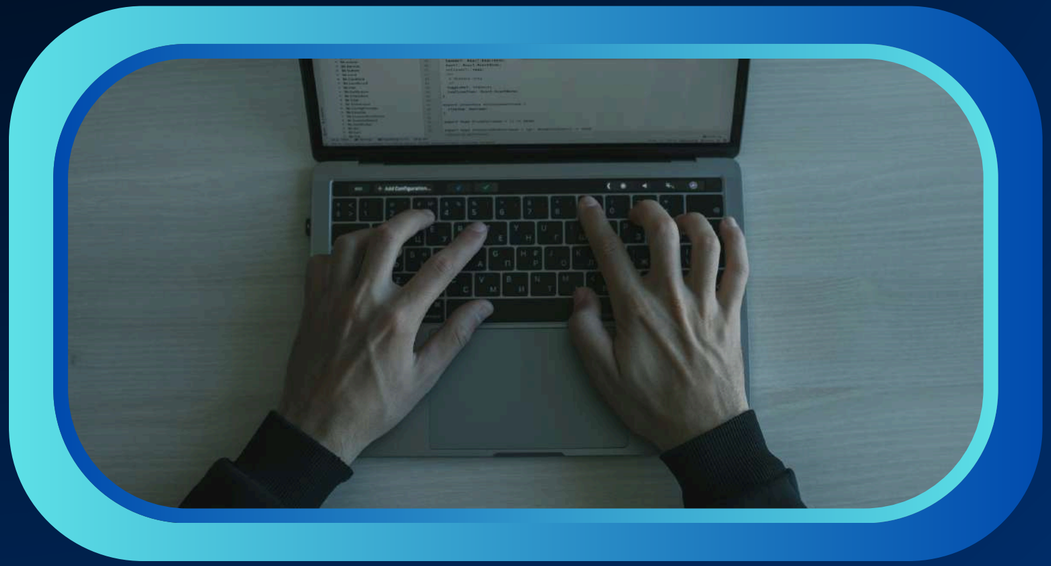
Аралас шифрлау әдісі (жылдамдық + қауіпсіз кілт алмасу) мен тиімді экспоненттi есептеу әдістерінің бірігуі қазіргі заманғы криптографиялық жүйелердің жоғары өнімділігі мен қауіпсіздігін қамтамасыз етеді.
Бұл әдістер заманауи ақпараттық қауіпсіздік жүйелерінің негізін құрайды.
Болашақта кванттық есептеулердің дамуы бұл әдістерді одан әрі жетілдіруді талап етеді.



БАҚЫЛАУ СҰРАҚТАРЫ

Аралас шифрлау әдісінің негізгі артықшылықтарын түсіндіріңіз.
Бинарлық әдіспен экспонентті есептеу қалай жүзеге асырылады?
Кватернарлық және октальды әдістердің айырмашылықтарын салыстырыңыз.
Симметриялы және асимметриялы криптожүйелердің кілт ұзындықтары неге әртүрлі болады?

ҰСЫНЫЛҒАН ӘДЕБИЕТТЕР:



1. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice
3. Paar, C., & Pelzl, J. (2010). Understanding Cryptography
4. Адамбеков, А. (2020). Ашық кілтті криптожүйелер және симметриялық криптографиялық алгоритмдер
5. Шнайер, Б. (2015). Криптография: практикалық қауіпсіздік шешімдері. Cryptography Engineering.
6. Фергюсон, Н., & Шнайер, Б. (2003). Криптографияның практикалық негіздері. Practical Cryptography.
7. Кнут, Д. Э. (1997). Компьютерлік бағдарламау өнері. 2-том. Жартылай сандық алгоритмдер. The Art of Computer Programming, Volume 2: Seminumerical Algorithms.

THANK YOU