# 10-ДӘРІС.
# ҚҰРАМДАС ШИФРЛАР

**SEC1811 «Ақпаратты криптографиялық қорғау негіздері»**

**Оқытушы: Ахмедиярова А.Т.**

# Дәрістің оқу нәтижелері

Дәріс соңында студент:

- құрамдас шифрды, блокты, раундты және раундтық кілтті анықтайды;
- шашырату мен араластырудың айырмасын түсіндіреді;
- XOR және қарапайым ауыстыру мысалдарын орындайды;
- көшкін әсерін есептейді;
- AES пен Фейстель желісінің жалпы архитектурасын салыстырады.

# Негізгі ұғымдар:

Ашық мәтін (M) — шифрланатын бастапқы ақпарат.

Шифрмәтін (C) — шифрлау нәтижесі.

Кілт (K) — түрлендіруді басқаратын құпия параметр.

Блоктық шифр — бекітілген ұзындықтағы биттер блогын өңдейтін шифр.

Құрамдас шифр — бірнеше қарапайым түрлендіруді тізбектеп біріктіретін шифр.

# Негізгі ұғымдар:

Ауыстыру (substitution) — символдың немесе биттер тобының мәнін өзгерту.

Орын алмастыру (permutation) — мәндерді сақтап, орындарын өзгерту.

XOR ($\oplus$) — биттер әртүрлі болса 1, бірдей болса 0.

Раунд — қайталанатын өңдеу кезеңі.

Раундтық кілт ($K_i$) — белгілі раундта қолданылатын кілт.

# XOR операциясы: ақиқат кестесі

$0 \oplus 0 = 0$ $0 \oplus 1 = 1$

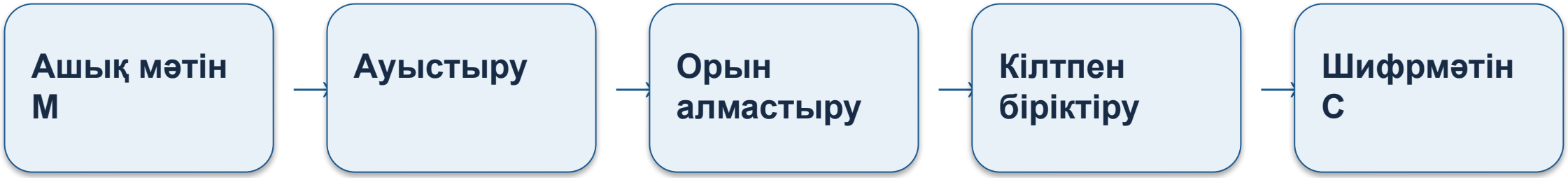
$1 \oplus 0 = 1$ $1 \oplus 1 = 0$

Мысал: $10110110 \oplus 01101001 = 11011111$

Маңызды қасиет: $(X \oplus K) \oplus K = X$.

Бір кілтті қайта XOR қолдану бастапқы биттерді қалпына келтіреді.

# Құрамдас шифрдың жалпы сұлбасы




Түрлендірулер бірнеше рет қайталануы мүмкін; нақты реттілік шифрға байланысты.

# Оқу мысалы: екі операцияның композициясы

1. Бастапқы блок: ABCD.
2. Әр әріпті әліпбидегі келесі әріпке ауыстыру: BCDE.
3. Екі жұптың орнын ауыстыру: DEBC.

Ауыстыру мәндерді өзгертеді; орын алмастыру позицияларды өзгертеді.

Бұл — түсіндіруге арналған мысал, қауіпсіз стандартты шифр емес.

# Шашырату (diffusion) дегеніміз не?

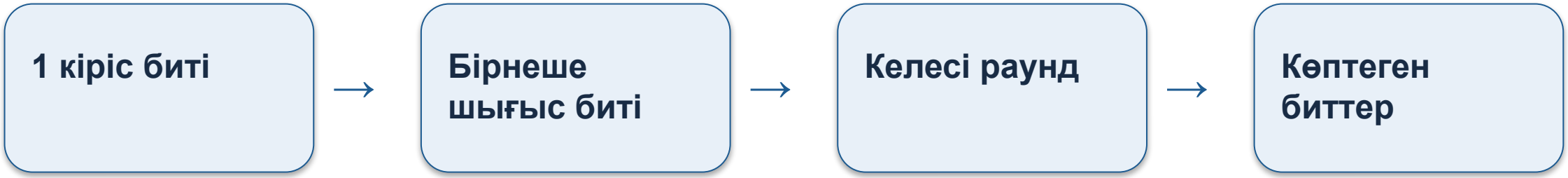
***Анықтама***: кірістегі бір биттің әсерін шығыстың көптеген биттеріне тарату қағидасы.

***Мақсаты***: бастапқы мәтіннің статистикалық заңдылықтарын шифрмәтінде байқатпау.

***Әдістер***: орын алмастыру, биттерді/байттарды араластыру, сызықтық түрлендірулер.

Мысал: $x_1$ өзгерсе, $y_1=x_1 \oplus x_2$ және $y_4=x_4 \oplus x_1$ өзгереді.

# Шашыратудың әсері




Шашырату бір раундта толық қалыптаспайды; өзгеріс бірнеше раунд бойы таралады.

# Араластыру (confusion) дегеніміз не?

***Анықтама***: кілт пен шифрмәтін арасындағы математикалық тәуелділікті күрделендіру қағидасы.

***Негізгі құрал:*** сызықтық емес ауыстыру (S-box).

Қарапайым $C=M \oplus K$ байланысының орнына сызықтық емес түрлендірулер қосылады.

***Мақсат***: кілттің шығысқа әсерін қарапайым формуламен сипаттауды қиындату.

# S-box: ауыстыру кестесі

Кіріс → Шығыс

00 → 10

01 → 00

10 → 11

11 → 01

Мысал: 01 кірісінің шығысы 00.

Ескерту: бұл кішкентай кесте тек ауыстыру идеясын көрсетеді; сызықтық еместік пен криптографиялық беріктік бөлек тексеріледі.

# Шашырату мен араластыру: салыстыру

***Шашырату***: ашық мәтін әсерін бүкіл блокқа таратады.

Негізгі тәсілдер: орын алмастыру, сызықтық араластыру.

***Араластыру***: кілт пен шығыс арасындағы байланысты күрделендіреді.

Негізгі тәсіл: сызықтық емес ауыстыру.

Қазіргі шифрларда екі қағида бірге жұмыс істейді.

# Раунд ұғымы және формуласы

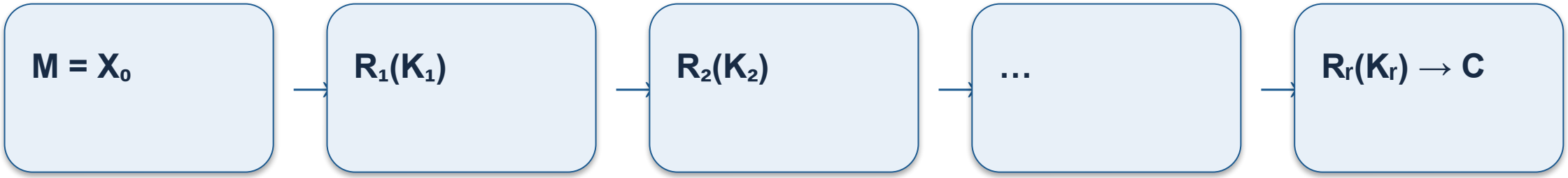
***Раунд*** — бірнеше криптографиялық операцияның қайталанатын жиынтығы.

$X_i = R(X_{i-1}, K_i), \quad i = 1, \ldots, r$

$X_0 = M$ — ашық мәтін; $R$ — раунд функциясы; $K_i$ — раундтық кілт; $X_i$ — раунд нәтижесі; $X_r = C$ — шифрмәтін.

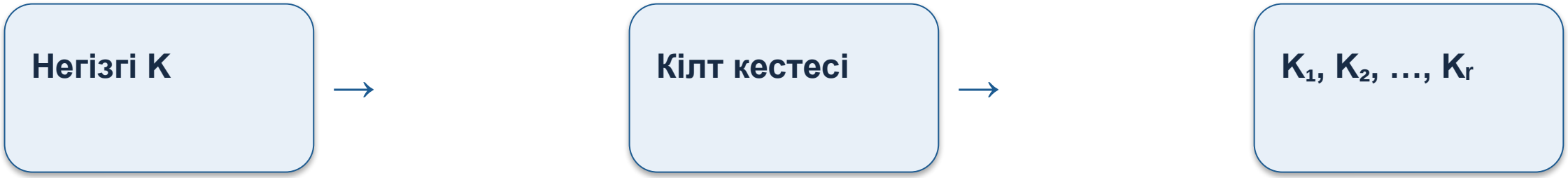
Раунд саны ғана емес, функцияның сапасы да маңызды.

# Көпраундты өңдеу архитектурасы




Әр раунд алдыңғы раундтың шығысын қабылдайды; кілттер негізгі құпия кілттен алынады.

# Раундтық кілттерді кеңейту




Кілт кестесі (key schedule) негізгі кілттен раундтарға қажетті кілт материалын шығарады.

# Раунд ішіндегі операциялар

Оқу үлгісі:

1. AddRoundKey: $X \oplus K_i$ — кілтпен біріктіру.
2. Substitution: S(X) — мәндерді ауыстыру.
3. Permutation / mixing — биттерді немесе байттарды тарату.
4. Нәтижені келесі раундқа беру.

Нақты стандарттарда қадамдардың құрамы мен реті өзгеше болуы мүмкін.

# Көшкін әсері (avalanche effect)

Анықтама: кірістегі немесе кілттегі бір биттің өзгеруі шығыста көптеген биттің өзгеруіне әкеледі.

Өзгеру үлесі: $A = (d / n) \times 100\%$

мұнда d — екі шифрмәтіндегі әртүрлі бит саны, n — блок ұзындығы.

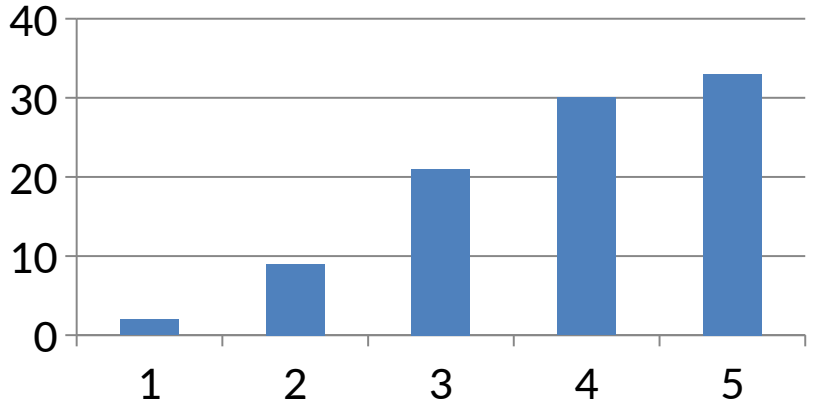
Мысал: $n=64$, $d=31 \rightarrow A=31/64\times100\%=48{,}4375\%$.

# Көшкін әсері: графикке арналған деректер

Төмендегі мәндер — оқу үшін алынған шартты мысал, AES өлшеулері емес.

| Раунд саны | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Өзгерген бит | 2 | 9 | 21 | 30 | 33 |

Блок ұзындығы: 64 бит.




Бірнеше раундтан кейін өзгерген биттер саны артуы мүмкін; әр нақты алгоритм экспериментпен тексеріледі.

# Көшкін әсерін бағалау алгоритмі

1. Бастапқы M блогын және K кілтін таңдау.
2. $C_1 = E(K, M)$ есептеу.
3. M блогының дәл бір битін өзгертіп M′ алу.
4. $C_2 = E(K, M')$ есептеу.
5. $d = C_1 \oplus C_2$ мәніндегі 1-биттер санын табу.
6. $A = 100d/n$ формуласымен үлесін есептеу.
7. Әртүрлі биттер мен блоктар үшін қайталау.

# AES: нақты блоктық шифрдың архитектурасы

AES — 128 биттік блоктармен жұмыс істейтін симметриялық шифр.

Кілт ұзындығы: 128, 192 немесе 256 бит.

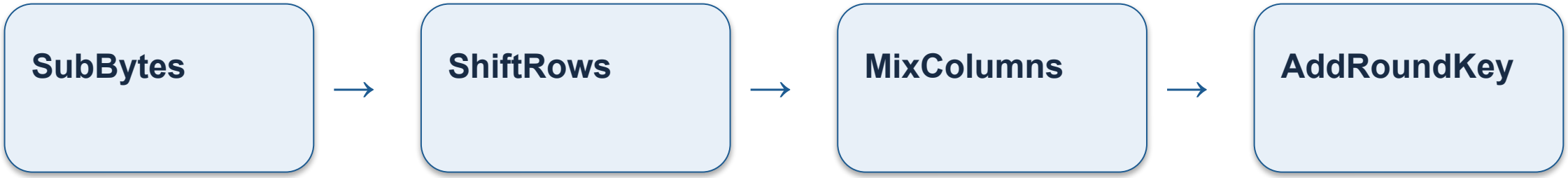
Раунд саны тиісінше: 10, 12 немесе 14.

Негізгі кезеңдер: SubBytes (S-box), ShiftRows, MixColumns, AddRoundKey.

Соңғы раундта MixColumns қолданылмайды.

AES — ауыстыру-орын алмастыру желісінің (SPN) мысалы.

# AES раундының ықшам сұлбасы




SubBytes — сызықтық емес ауыстыру; ShiftRows пен MixColumns — шашырату; AddRoundKey — кілтпен XOR.

# Фейстель желісі: негізгі идея

Блок екі жартыға бөлінеді: $L_i$ және $R_i$.

$L_{i+1} = R_i$

$R_{i+1} = L_i \oplus F(R_i, K_i)$

F — раунд функциясы; $K_i$ — раундтық кілт.

Фейстель құрылымында кері түрлендіруді раунд кілттерін кері ретпен қолдану арқылы ұйымдастыруға болады. DES — тарихи мысал.

# AES пен Фейстель желісін салыстыру

AES (SPN): бүкіл блок күйі бірқатар ауыстыру және араластыру қадамдарынан өтеді.

Фейстель: блок екі жартыға бөлініп, раунд функциясы мен XOR арқылы өңделеді.

Ортақ белгілер: көпраундты құрылым, раундтық кілттер, шашырату және араластыру.

Айырмашылығы: деректердің раунд ішіндегі қозғалысы мен кері түрлендіру тәсілі.

# Тарихи деректер

1949 жылы Клод Шеннон «Communication Theory of Secrecy Systems» еңбегінде confusion және diffusion ұғымдарын жүйеледі.

1970-жылдары IBM зерттеушілері, соның ішінде Хорст Фейстель, блоктық шифрлардың дамуына ықпал етті.

1977 жылы DES федералдық стандарт ретінде бекітілді.

2001 жылы AES стандарты қабылданды; ол Rijndael алгоритміне негізделген.

# Криптографияда қолданылу ерекшелігі

Құрамдас шифрлар файлдарды, деректер ағындарын және байланыс арналарының ақпаратын қорғауда қолданылады.

Шифрдың өзі жеткіліксіз: дұрыс жұмыс режимі, бірегей nonce/IV, кілтті қауіпсіз сақтау және тұтастықты қорғау қажет.

Практикада AES-GCM сияқты аутентификацияланған шифрлау режимдері жиі қолданылады.

Оқу мысалдарын нақты деректерді қорғауға қолдануға болмайды.

# Шешілген есеп: XOR және өзгерген биттер

$M_1$ = 10110010; $M_2$ = 10110011.

$M_1 \oplus M_2$ = 00000001 → айырмашылық 1 бит.

Екі 8-биттік шартты шифрмәтін берілсін:

$C_1$ = 11001010; $C_2$ = 00110110.

$C_1 \oplus C_2$ = 11111100 → d = 6.

A = (6/8)×100% = 75%.

Бұл шифрмәтіндер нақты алгоритммен есептелмеген, шартты мысал.

# Практикалық тапсырмалар

1. 11001010 $\oplus$ 10110101 мәнін есептеңіз.
2. ABCD $\rightarrow$ BCDE $\rightarrow$ DEBC мысалындағы екі операцияны атаңыз.
3. Шашырату мен араластыруға екі мысал келтіріңіз.
4. 128 биттік екі шифрмәтіннің 61 биті өзгеше: A мәнін табыңыз.
5. AES-128 неше раундтан тұрады?
6. Фейстель желісіндегі $L_{i+1}$ және $R_{i+1}$ формулаларын түсіндіріңіз.

# Бақылау сұрақтары

1. Құрамдас шифр дегеніміз не?
2. Ауыстыру мен орын алмастырудың айырмашылығы?
3. Шашырату дегеніміз не?
4. Араластыру дегеніміз не?
5. Раунд пен раундтық кілт не үшін керек?
6. Көшкін әсері қалай өлшенеді?
7. AES архитектурасында қандай қадамдар бар?
8. Фейстель желісінің ерекшелігі қандай?
9. Раунд санын көбейту неге жеткіліксіз?
10. Шифрды қолдануда қандай қосымша қауіпсіздік шарттары маңызды?

# Қорытынды

Құрамдас шифр қарапайым операцияларды біріктіріп, оларды бірнеше раунд бойы қайталайды.

Шашырату — бір кіріс өзгерісінің әсерін көптеген шығыс позицияларына таратады.

Араластыру — кілт пен шифрмәтін арасындағы тәуелділікті күрделендіреді.

Көшкін әсері — осы қасиеттерді тәжірибелік бағалаудың бір көрсеткіші.

Қауіпсіздік раунд санына ғана емес, алгоритм архитектурасы мен қолдану тәсіліне тәуелді.