11-ДӘРІС. СИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕЛЕР ЖӘНЕ ФЕЙСТЕЛЬ ЖЕЛІСІ

Құру принциптері

- Блоктық және ағындық шифрлар
- Раундтық түрлендірулер

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің оқу нәтижелері

- Симметриялық криптожүйенің жұмыс принципін түсіндіру
- Блоктық және ағындық шифрларды салыстыру
- Фейстель раундының теңдеулерін қолдану
- Шифрлау мен кері түрлендіруді есептеу
- Кілттерді басқару мен шифр жобалау шарттарын талдау

Негізгі ұғымдар

Симметриялық криптожүйе — шифрлау және дешифрлау үшін ортақ құпия кілт қолданатын жүйе.

Ашық мәтін (M) — бастапқы хабарлама.

Шифрмәтін (C) — шифрланған хабарлама.

Құпия кілт (K) — түрлендіруді анықтайтын параметр.

Шифрлау E_k және дешифрлау D_k — өзара кері операциялар.

Шифрлау және дешифрлау формулалары

$C = E_k(M)$

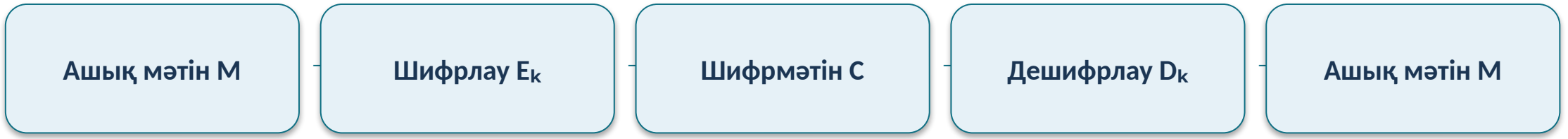
$M = D_k(C)$

$D_k(E_k(M)) = M$

Кілт құпия сақталуы тиіс; байланыс арнасымен шифрмәтін жіберіледі.

Симметриялық байланыстың архитектурасы

Жіберуші мен қабылдаушы бір құпия кілтке ие.



Артықшылықтары мен шектеулері

Артықшылықтары:

• Жоғары өнімділік; үлкен көлемді ақпаратты өңдеу

• Файлдар, деректер қоры және желілік трафик үшін жарамды

Шектеулері:

• Кілтті қауіпсіз жеткізу қажет

• Кілттерді сақтау, жаңарту және жою қажет

• Пайдаланушылар көбейген сайын басқару қиындайды

Кілттер саны: есеп

Егер әр пайдаланушы жұбына жеке ортақ кілт қажет болса:

$N = n(n - 1) / 2$

Мысал: $n = 10 \rightarrow N = 10 \times 9 / 2 = 45$ кілт.

Егер $n = 20$ болса $\rightarrow N = 20 \times 19 / 2 = 190$ кілт.

Ескерту: бұл толық жұптық байланыс моделі.

Симметриялық шифрлардың түрлері

Ағындық шифр — биттерді/байттарды кілттік ағынмен өңдейді.

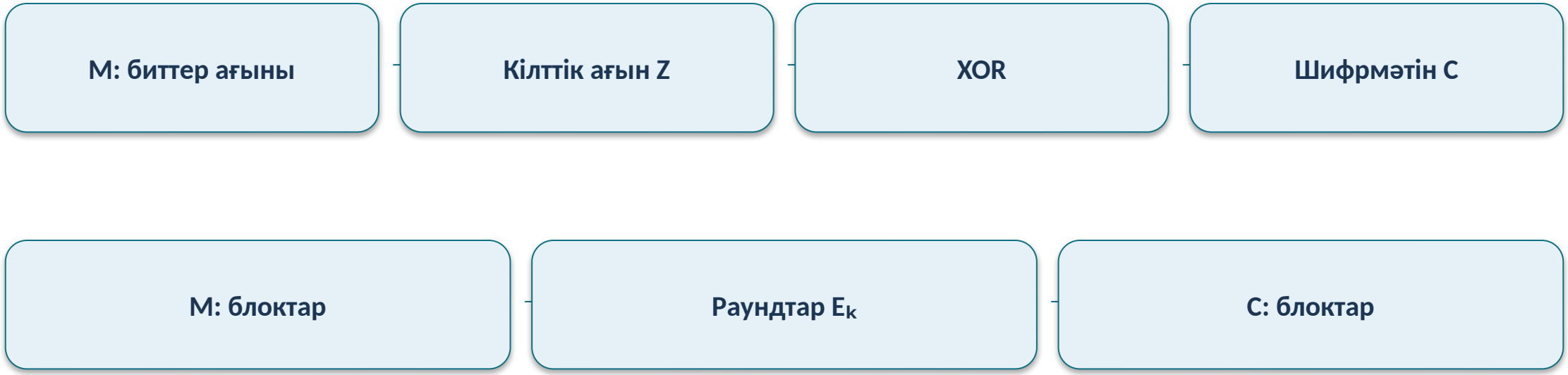
Блоктық шифр — бекітілген ұзындықтағы блоктарға түрлендіру қолданады.

Ағындық: $c_i = m_i \oplus z_i$

Блоктық: $C_i = E_k(M_i)$

Ағындық және блоктық тәсіл: сұлба

Екі тәсілдің өңдеу бірлігі әртүрлі.



Ағындық шифр: XOR мысалы

Ашық мәтін: 10110010

Кілттік ағын: 01101100

Шифрмәтін: 11011110

Кері есептеу: 11011110 ⊕ 01101100 = 10110010

Бұл — XOR қағидасының оқу мысалы, толық қауіпсіз шифр емес.

Блоктық шифрдың құрамы

Блок бірнеше раундтан өтеді.

Раундтарда XOR, ауыстыру, орын алмастыру, сызықтық және сызықтық емес түрлендірулер болуы мүмкін.

Мақсат: араластыру (confusion) мен шашыратуды (diffusion) қамтамасыз ету.

10-дәрісте қарастырылған AES — SPN құрылымының мысалы.

Фейстель желісі: анықтама

Фейстель желісі — блокты сол (L) және оң (R) жартыға бөліп, әр раундта функция мен XOR арқылы өңдейтін көпраундты құрылым.

$X_0 = (L_0, R_0)$

F — раундтық функция; K_i — i-раундтың кілті.

Фейстель раундының теңдеулері

$L_i = R_{i-1}$

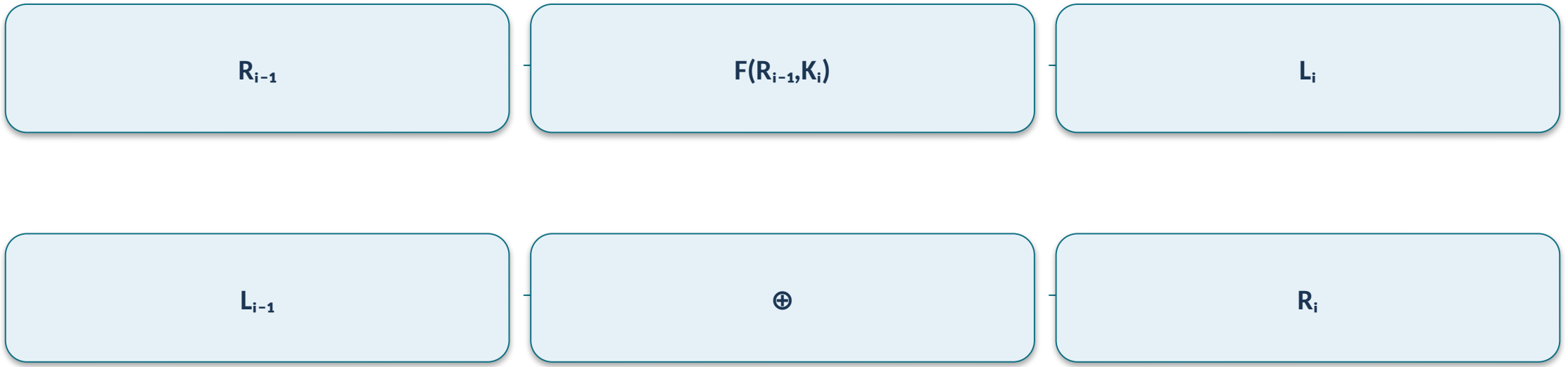
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Бұрынғы оң бөлік жаңа сол бөлік болады.

F нәтижесі бұрынғы сол бөлікпен XOR арқылы біріктіріледі.

Фейстель раундының құрылымдық сұлбасы

Бір раундтағы деректер қозғалысы:



Бір раунд: толық шешілген мысал

Берілгені: $L_0 = 1010$; $R_0 = 0110$; $F(R_0,K_1) = 1100$.

1) $L_1 = R_0 = 0110$.

2) $R_1 = L_0 \oplus F(R_0,K_1)$.

3) $R_1 = 1010 \oplus 1100 = 0110$.

Жауап: $(L_1,R_1) = (0110,0110)$.

Көпраундты өңдеу алгоритмі

1. Блокты L_0 және R_0 жартысына бөлу.

2. i = 1, 2, …, r үшін:

   $T = F(R_{i-1}, K_i)$

   $L_i = R_{i-1}$

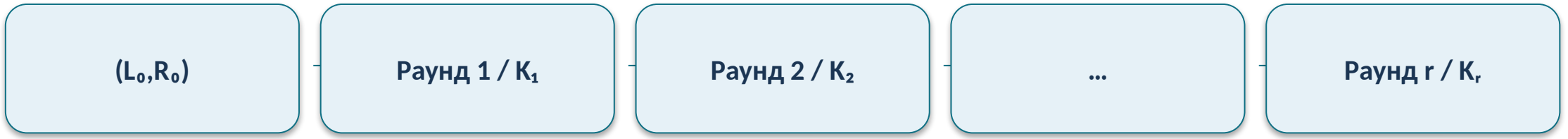
   $R_i = L_{i-1} \oplus T$

3. Соңғы (L_r, R_r) күйін шығару.

Раундтық кілттер негізгі кілттен туындатылады.

Көпраундты Фейстель желісі

Әр раунд алдыңғы раунд нәтижесін қабылдайды.



Неліктен Фейстель желісі қайтымды?

F функциясының өзі кері функцияға ие болуға міндетті емес.

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus F(L_i, K_i)$

Негіздеме: $A \oplus B \oplus B = A$.

Осы теңдеулер алдыңғы раундты дәл қалпына келтіреді.

Кері түрлендіру: шешілген мысал

Раунд нәтижесі: $(L_1,R_1) = (0110,0110)$.

$F(L_1,K_1) = 1100$.

1) $R_0 = L_1 = 0110$.

2) $L_0 = R_1 \oplus F(L_1,K_1)$.

3) $L_0 = 0110 \oplus 1100 = 1010$.

Бастапқы блок: (1010,0110).

Раундтық кілттердің реті

Төрт раундтың мысалы:

Шифрлау	K_1	K_2	K_3	K_4
Дешифрлау	K_4	K_3	K_2	K_1

Шифрлау және дешифрлау: салыстыру

Шифрлау: $K_1 \rightarrow K_2 \rightarrow \ldots \rightarrow K_r$.

Дешифрлау: $K_r \rightarrow \ldots \rightarrow K_2 \rightarrow K_1$.

Негізгі раундтық операциялар қайта қолданылады; жарты блоктардың ретін өңдеу нақты іске асыруға байланысты.

Артықшылық: аппараттық және бағдарламалық іске асыруды ықшамдау.

Фейстель желісін құру принциптері

- Блок пен кілт ұзындығын таңдау
- Раунд санының жеткіліктілігін бағалау
- F функциясының сызықтық еместігі
- Раундтық кілттерді генерациялау сапасы
- Белгілі криптоталдау әдістеріне төзімділік
- Қауіпсіз жұмыс режимі және кілттерді басқару

Тарихи және практикалық контекст

Хорст Фейстельдің зерттеулері блоктық шифрлардың дамуына ықпал етті.

DES — Фейстель құрылымының тарихи мысалы.

AES — басқа құрылымға (SPN) негізделген.

Нақты деректерді қорғау үшін оқу үлгілерін емес, тексерілген стандарттар мен дұрыс қолдану режимдерін пайдалану қажет.

Практикалық тапсырмалар

1. 11010110 ⊕ 01100101 мәнін есептеңіз.
2. n = 15 пайдаланушыға қанша жұптық кілт қажет?
3. L_0=1101, R_0=0011, $F(R_0,K_1)$=1010 үшін бір раундты есептеңіз.
4. Алынған нәтижеден бастапқы блокты кері қалпына келтіріңіз.
5. Ағындық және блоктық шифрдың екі айырмашылығын атаңыз.

Бақылау сұрақтары

1. Симметриялық криптожүйе дегеніміз не?
2. Ортақ кілтті басқару неге күрделі?
3. Ағындық және блоктық шифрлардың айырмасы қандай?
4. Фейстель раунды қалай орындалады?
5. F функциясының рөлі қандай?
6. Фейстель құрылымы неліктен қайтымды?
7. Дешифрлау кезінде кілттер қалай қолданылады?
8. Раунд саны не үшін маңызды?
9. Кілт кестесінің міндеті қандай?
10. Шифр жобалауда қандай факторлар ескеріледі?

Қорытынды

Симметриялық криптожүйе ортақ құпия кілтке негізделеді.

Ағындық шифр деректерді біртіндеп, блоктық шифр бекітілген блоктармен өңдейді.

Фейстель желісі екі жарты блокты F және XOR арқылы байланыстырады.

Кері түрлендіру XOR қасиетімен қамтамасыз етіледі.

Жүйенің қауіпсіздігі алгоритмге ғана емес, кілттерді дұрыс басқаруға да байланысты.

Әдебиеттер

1. Ахметов Б.С. және т.б. Қолданбалы криптология: шифрлау әдістері. Алматы, 2016.
2. Ахметов Б.С. және т.б. Криптография негіздері. Алматы, 2020.
3. Васильева И.Н. Криптографические методы защиты информации. Юрайт, 2024.
4. Лось А.Б. және т.б. Криптографические методы защиты информации. Юрайт, 2024.
5. Омассон Ж.-Ф. О криптографии всерьез. ДМК Пресс, 2021.