

Дәріс 2. Негізгі қол шифрлары

Дәріскер: PhD Темирбекова Ж.Е.

Дәріс жоспары:

- ▶ Цезарь шифры
- ▶ Тритемий шифры
- ▶ Виженер шаршысы
- ▶ Плейфер шифры
- ▶ «Қос шаршы» әдісі

Цезарь шифры

- Ауыстыру шифры, формулалар, мысал және кестелік әдіс.

$$\text{егер } c \leq n, c = a + k,$$

$$\text{егер } c > n, c = a + k - n.$$

Мұндағы k саны криптографиялық жүйенің кілті деп аталады.

Цезарь шифрінің мағынасы ашық мәтіннің кез келген әрпі өзіне қатысты k әріппен ауыстырылады.

Мысал. k кілті 7-ге тең болсын, сонда *алфавит* сөзі Цезарь шифры арқылы *зжзж* сөзіне айналады. *б* әрпінің коды 2, ал *а* әрпінің коды 1, *з* және *ж* әріптері *б* және *а*-ға қатысты жеті позицияға жылжытылады. Содан кейін шифрланған жазбаның әріптік кодтары келесідей анықталады:

$b+k = 2+7 = 9$ саны *з* әрпіне, ал $a + k = 1+7 = 8$ саны *ж* әрпіне сәйкес келеді.

Тритемий шифры

- Көпалфавиттік ауыстыру, Тритемий кестесі.

$$\gamma = \alpha + k$$

Бұл формула α әрпінің пайда болу жиілігін γ белгісінің пайда болу жиілігіне автоматты түрде «тасымалдайды». Нәтижесінде, шифрланған мәтінді талдау кезінде үлгілер мен жиілік сипаттамаларын анықтауға болады, бұл қарапайым ауыстыру шифрын криптоанализге осал етеді.

Виженер шаршысы

- Циклдік алфавиттер, кілтпен шифрлау ережесі.

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯА
ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
ГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
ДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГ
ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД
ЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕ
ЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖ
ИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗ
КЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИ
ЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИК
МНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛ
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ
ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМН
ПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНО
РСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОП
СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР
ТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРС
УФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТ
ФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУ
ХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФ
ЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХ
ЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦ
ШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧ
ЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШ
ЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩ
ЫЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪ
ЬЭЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫ
ЮЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ
ЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭ
ЯАБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮ

Шифрлау кестелері

- Сциталь, оқу бағыттары, мысал кестелер.

	1	2	3	4
1	П	Р	И	Е
2	З	Ж	А	Ю
3	α	Ш	Е	С
4	Т	О	Г	О

Плейфер шифры

- Биграммалар, кестемен алмастыру ережелері.

Плейфер шифры үшін $N = n \times t$ өлшемді кесте құрылады. Мұнда n жолдар саны, t бағандар саны. N саны әліпбидегі таңбалар санына сәйкес келуі керек. Кестедегі алфавит таңбалары кездейсоқ реттелген. Кестенің өлшемі және ондағы белгілердің орналасуы осы криптографиялық жүйенің кілті болып табылады.

«Қос шаршы» әдісі

- ▶ Екі кесте, биграммалар, жоғары тұрақтылық.
- ▶ «Қос шаршы» әдісі үшін $N = n \times t$ өлшемді екі кесте құрылады, мұндағы n жолдар саны, t бағандар саны. N кестелеріндегі элементтер саны алфавиттегі таңбалар санына сәйкес келуі керек. Кестелердегі алфавит таңбалары кездейсоқ орналасады және олардың реті алфавитке сәйкес келмеуі керек. Кестелердің өлшемдері және олардағы таңбалардың орналасуы берілген криптографиялық жүйенің кілті болып табылады. Бір кесте сол (нөмір 1), екіншісі оң (нөмір 2) деп аталады.

Қолданылған әдебиеттер

- ▶ 1. Кац Дж., Линделл Ю. Введение в современную криптографию. / Кац Дж. - М.: Триумф, 2018. - 342 с.
- ▶ 2. Бонех Д., Шуп В. Аспирантура по прикладной криптографии. / Бонех Д. - Спрингер, 2020. - 514 с.
- ▶ 3. Менезес А., Ван О., Ванстон С.А. Справочник по прикладной криптографии. / Менезес А. - ЦРК: Пресс, 2018. - 516 с.