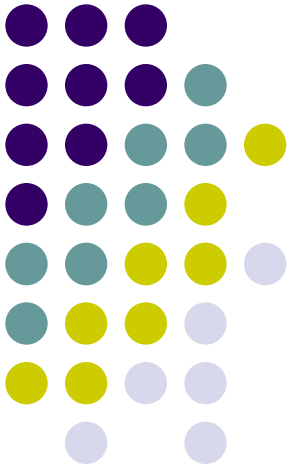
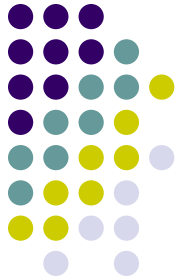
Ағымды шифрлер

Дәріс 7

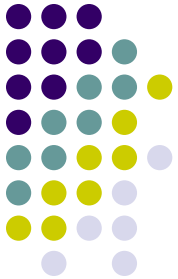




- Ағымды шифрлер гаммалау түрін көрсетеді

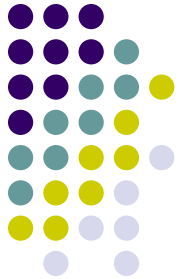
- Ағымды шифрлер деректердің үзіліссіз ағынын шифрлеу үшін қолданылады, мысалы деректерді желілерде жіберу.

Ағымды шифрлер



- - бұл ашық мәтін элементтерімен түрлендірулерді тізбектей орындауға арналған криптожүйелер
- Сондай-ақ ашық мәтін элементтері кішігірім өлшемге ие.
- Мұндай элементтер табиғи тіл алфавитінің әрпі немесе хабарламаның 1 биті болып табылады.

Ағымды шифрдің жалпы схемасы



- **Кілттік тізбек генераторы, (жүгірмелі кілт генераторы)**

к1, к2, ..., ki ... бит тізбегін береді

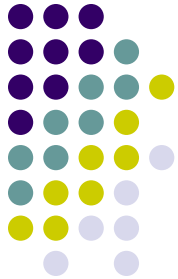
- **Кілттік тізбек шифрмәтін алу үшін p1,p2, ...,pi ... алғашқы мәтіннің тізбегімен 2 модулі бойынша қосылады**

$$Ci=Pi \oplus Ki$$

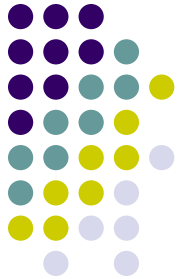
- **Қабылдаушы жақта шифрленген мәтін 2 модулі бойынша шифмәтінді алу үшін бірдей кілттік тізбекпен қосылады.**

$$Ci \oplus Ki = Pi \oplus Ki \oplus Ki = Pi$$

Ағымды шифрлердің төзімділігі

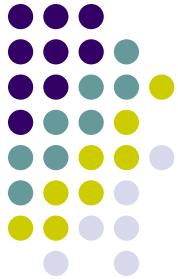


- Жүйенің төзімділігі кілттік тізбек генераторының ішкі құрылымына толықтай тәуелді.
- Егер генератор кішігірім периодпен тізбекті берсе, онда жүйенің төзімділігі жоғары болмайды
- Төзімділікті ұлғайту үшін барлық ағымды шифрлер кілттік тізбек генерациясы үшін кілтті қолдануды қарастырады.



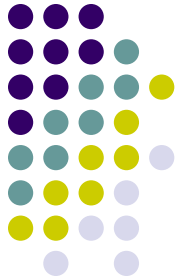
- Поточные
- шифры
  - Самосинхрони-
  - зирующиеся
  - Синхронные

Өзіндік синхрондалатын шифрлер (автокілтпен)



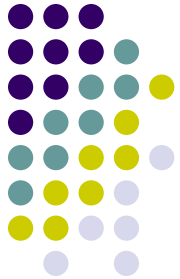
- Генератордың ішкі жағдайы шифрленген мәтіннің алдыңғы биттерінің тіркелген сан функциясы болып табылады.
- Ішкі жағдай шифрленген мәтіннің **n** битіне байланысты болғандықтан генератор қабылдаушы жақта **n** битті алған соң жіберуші жақпен синхронизмге кіреді.
- **Осы бағытты жүзеге асыру**:
  - Әрбір хабарлама **n бит** ұзындығымен кездейсоқ тақырып жолымен алынады.
  - Бұл тақырып жолы шифрленеді және линиямен жіберіледі.
  - Қабылдаушы жақта тақырып жолы дешифрленеді.
  - Дешифрлеу нәтижесі қате болады, бірақ **n** бит тақырып жолын өңдеген соң екі генератор да синхрондалады.

Өзіндік синхрондалатын шифрлердің кемшіліктері



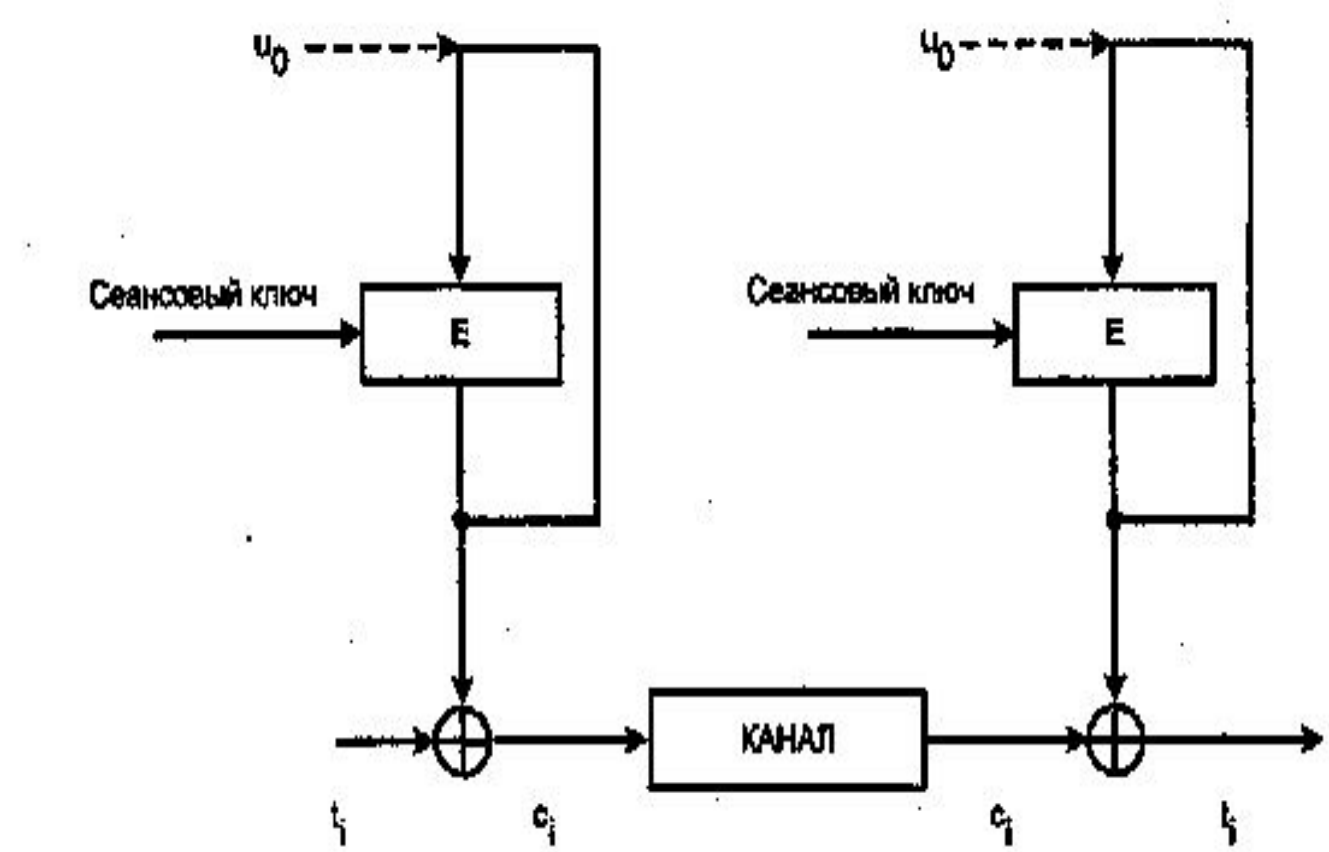
- **Қатені тарату**.
  Бір биттің тежелуі кезінде қабылдаушы жақтағы генератор кілттік тізбектің **n** қате битін береді.
- **«Воспроизведение»** типті шабуылға **төзімсіз**.
  - Қаскүнем шифрленген мәтіннің қандайда бір бит санын жазады.
  - Содан, біраз уақыттан соң ол трафик битін жазылған деп ауыстырады– оларды "воспроизводит».
  - Қабылдаушы жақ синхрондалмағанша қандайда бір “қоқыс” санынан соң ескі шифрленген мәтін дұрыс дешифрленеді.
  - Қабылдаушы жақта қабылданатын деректер актуалды болып табылмайтындығын анықтаудың ешқандай әдістері жоқ.

Өзіндік синхрондалатын ағымды шифрлер



- Шифрленген мәтін бойынша кері байланыс режимінде қолданылатын блоктық шифрлер түрінде жүзеге асырылуы мүмкін
- Біз мезетте блоктың ұзындығынан кем немесе тең биттің дербес санын шифрлеуі мүмкін.

Шифрлеу функциясының кері байланысы бойынша қалыптастырылатын кілттік гаммамен ағымды шифр



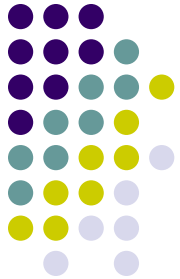
U_0 – инициализация көрсеткіші немесе векторы

T – алғашқы мәтін

C – шифрмәтін

E – шифрлеу функциясы

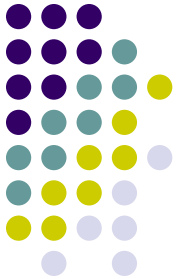
Шифрлеу функциясының кері байланысы бойынша қалыптастырылатын кілттік гаммамен ағымды шифр



- Кілттік ағын генерациясы блоктық шифр кірісіне инициализация көрсеткіші немесе векторы деп аталатын U_0 қандайда бір бастапқы мәнді берумен басталады.
- **Көрсеткіш** құпия кілтті қолданумен шифрленеді.
- Шығу блогынан енгізілетін мәтіннің бірінші битін (немесе бірінші элементін) түрлендіру үшін бір бит (немесе r бит) алынады.
- ал шығатын мәннің өзі блоктық шифр кірісіне беріледі және шифрленеді.
- Жаңа шығатын мән кілттік ағынның кезекті элементін береді және қайтадан блоктық шифрдің кірісіне беріледі және т.с.с.

Циклге бір байт бойынша шифрлеу мысалы

(8 саны мысал үшін ғана алынған)

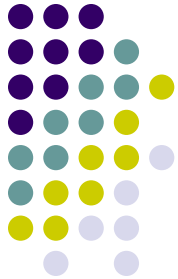


- Блоктық шифр блоктың ұзындығына тең өлшеммен жұмыс істейді.
- Алдымен кезек синхропосылкамен толтырылады.
- Содан соң кезек шифрленеді және сол жақтағы 8 бит алғашқы мәтіннің бірінші 8 битімен қосылады.
- Шифрленген мәтіннің алынған 8 биті линияға жіберіледі,
- Кезек сол жаққа 8 битке жылжиды, сол жақтағы биттер алынып тасталады, ал оң жақтағылар линияға жіберілген шифрленген мәтіннің 8 битімен толтырылады.
- Ары қарай процедура қайталанады.

Шектеулер:

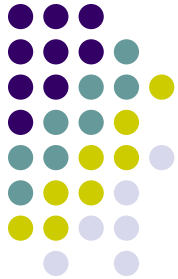
- CFB режимінде **синхропосылка** кілттің жұмыс істеу мерзімінде әрбір хабарлама үшін әмбебап болуы керек. Егер олай болмаса, қаскүнем алғашқы мәтінді қалпына келтіруі мүмкін.

Синхронды шифрлер



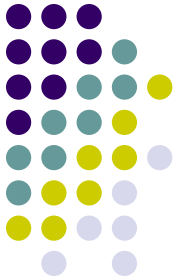
- Генератордың шығару мәндері алғашқы немесе шифрленген мәтінге байланысты емес.
- Берілген жағдайда негізгі қиындық жіберілетін және қабылдаушы жақтарда кілт генераторларының синхронизациясы қажеттілігінен тұрады.
- Егер жіберу процесінде бір бит болсын түсіп қалып немесе қойылса, онда шифрленген мәтін биттерінің барлық тізбегі қате биттен соң дешифрленбейді.
- Егер ондай жағдай болып қалса, онда жақтар қайта синхрондау жүргізу керек.
- Сондай-ақ синхрондау кілттік тізбектің ешқандай кескіні қайталанбайтындай жүргізілуі керек, демек генератордың қандайда бір алдыңғы жағдайына қайтып келу шешімі келмейді.

Артықшылықтары мен кемшіліктері



- **Қатені тарату эффектісінің жоқтығы**.
  Жіберу кезінде бір тежелген бит дешифрлеу кезінде мәтіннің тек бір битін тежеуге әкеледі.
- **Ағыннан шифрленген мәтін кескінін қою және алып тастаудан қорғайды.**
  Мұндай операциялар синхрондауды бұзуға әкеледі, ол дереу қабылдаушы жақта табылады.
- **Жеке биттердің өзгеруіне төзімсіз**.
  Егер зиянкес алғашқы мәтінді білсе, онда ол шифрленген мәтін ағынында биттерді өзгерте алады, зиянкеске қалай қажет, солай дешифрлейді.

Ағымды шифр мысалдары



- **RC4** алгоритмі- RSA Data Security, Inc компаниясы үшін 1987 ж. Рон Ривестпен құрастырылған кілттің айнымалы ұзындығымен ағымды шифр.
- **SEAL** алгоритмі- (Фил Рогвэй мен Дон Копперсмит)– 32-разрядты процессорлар үшін IBM фирмасымен құрастырылған ағымды шифр.
- **WAKE** алгоритмі - Дэвид Уилермен ұсынылған автокілтпен сөздерді шифрлеу