XIX ғасырдағы криптография

Орындаған: Бірмағанбет Сабина
Доспанова Нурайым
ИС 15-200-31 топ

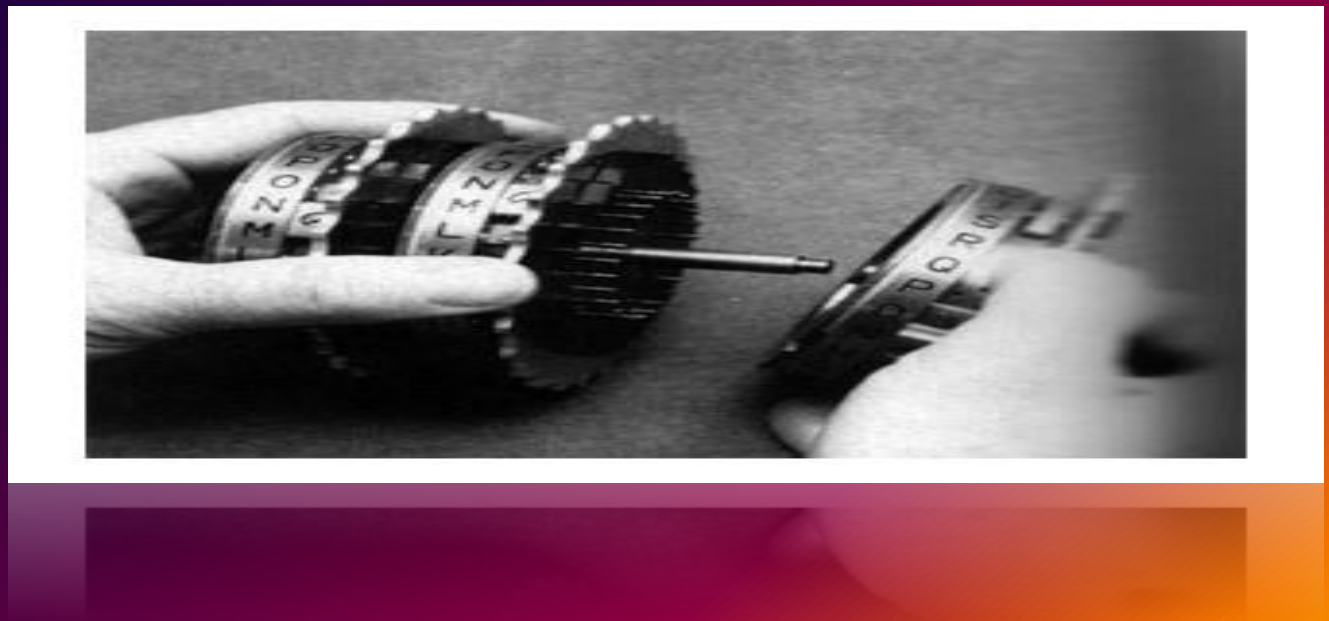
Жоспар:

1. XIX ғасырдағы криптография.
2. Ғылыми-технологиялық революция және оның криптографияға әсері
   - Телеграф
   - Радио
   - Телефон
3. Қорытынды.

Ғылым мен техниканың даму жетістіктері криптографияның дамуына үлкен әсер етеді.

XIX ғасырдың ортасында телеграфты ойлап тапқаннан кейін оны қолданатың бірнеше дипломатиялық және сауда шифрлері пайда болды. XIX ғасырдың аяғында механикалық Т.Джефферсон мен Ч.Уитстонның шифрлаторлары пайда болды. XX ғасырда ақпаратты үлкен қашықтыққа үлкен жылдамдықпен беруге жаңа мүмкіндіктер пайда болды. Алдымен криптография электрмеханикалық болып, сосын электронға ауысты.

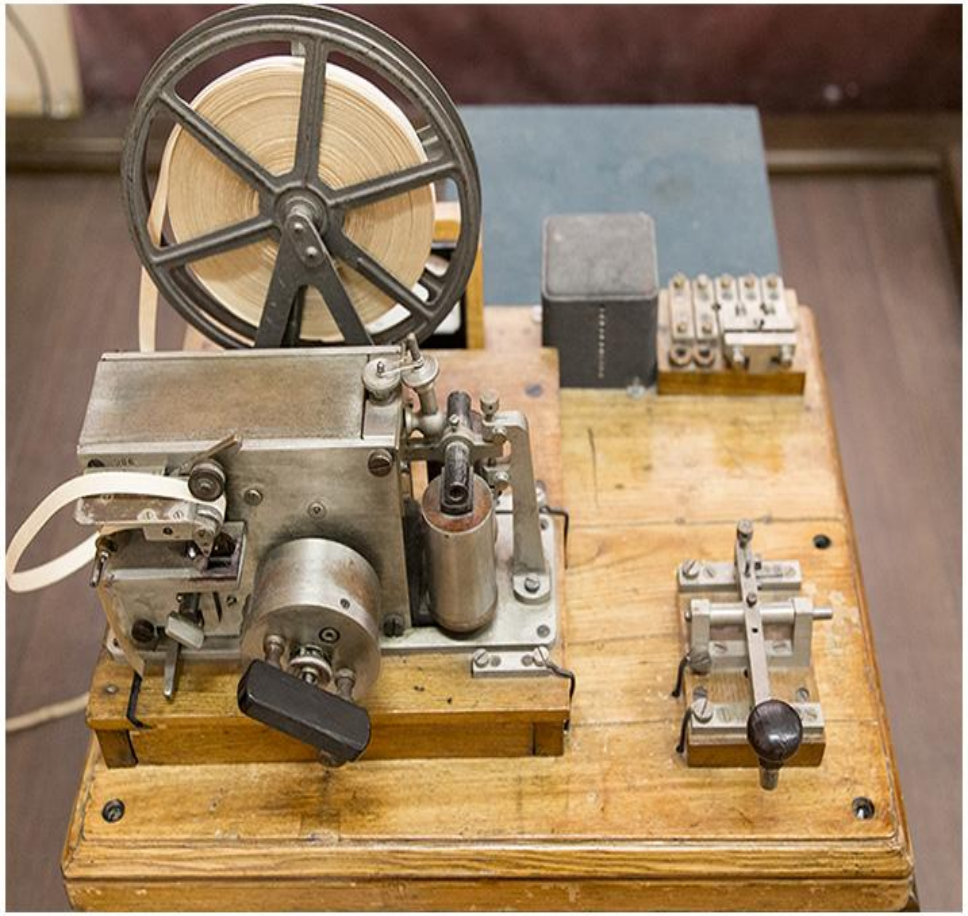
Криптография, жаңа дәуірден бірнеше ғасыр бұрын пайда болған ақпаратты қорғаудың ең қуатты құралы, оның басты мақсаты мәтінді кездейсоқ таңбалар жинағына айналдыру. XIX ғасырға дейін криптографияның өнер ретінде дамығаны және тек осы кезеңде ғана дәл математикалық ғылымның қасиеттеріне ие бола бастады. XIX ғасыр криптографияның тарихына ғылыми-техникалық прогрестің криптографияның шешілуіне қосқан елеулі үлесі ретінде кірді, оның дамуы айқын.

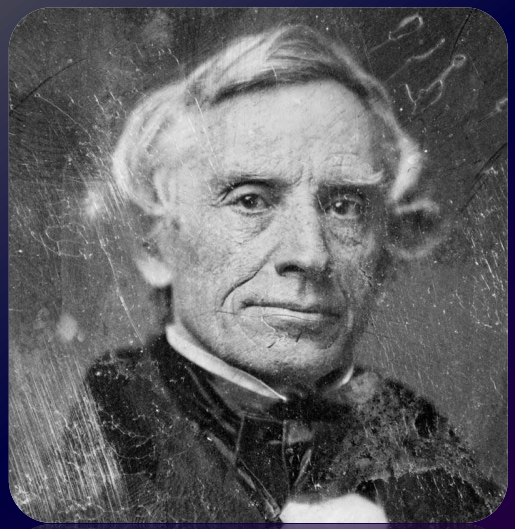


Ғылыми-технологиялық революция және оның криптографияға әсері

1. ТЕЛЕГРАФ

Ұзақ қашықтықтағы хабарларды жылдам хабарлау ежелгі уақытта пайда болды. Ондағы барабандар, түтін сигналдары, өрттер және т.б. сияқты қарапайым қарым-қатынас әдістері тиісті кодын қолдануды талап етті. Бұл кодтар байланыс желісі бойынша берілуге болатын нысанда ақпаратты беруге мүмкіндік берді. Тіпті ежелгі римдіктерде империя аумағы арқылы жарық сигналдарын беру үшін 3000-нан астам мұнара болған. **1794** жылы К.Чапп Париж мен Лилль арасында «әуе-телеграф» салған. Байланыстың негізгі элементі - **семафор**. Ақпаратты таратудың бұл жүйесі тиімді болып шықты және Францияда кеңінен таратылды. Ақпаратты **«жалауша кодтары»** арқылы жіберу кемелер арасындағы байланыс орнатуда қолдануды тапты.





Сэмюэл Морзе

Іс жүзінде қолданылатын **электромагниттік телеграфты** ресейлік азамат **П. Л. Шиллингом** құрды, көрнекті ғалым және өнертапқыш. Бұл құрылғыны ол **1832** жылдың қазан айында ашты. Оның әрекеті электр магниттік өрістердің электр сымдарының нәтижесінде магнитті иненің құлауының әсері болды. Бұл жағдайда таратушы және қабылдайтын аппараттар сегіз сымнан тұратын кабель арқылы қосылған. Әр сым беру кезінде өз кілті арқылы қосылды. Бұл жағдайда бір хат жіберу үшін бір мезгілде үш немесе төрт пернені басу қажет болды

1844 жылы С. Морзе әлемдегі алғашқы сымды телеграф арқылы: **«Вот что сотворил Бог!»,** деп ақпарат жіберді. Сол кезде Морзе «Морзе коды» деп аталатын хаттарды кодтау үшін арнайы алфавитті пайдаланды. 1845 жылы Ф. Смит адвокаты С. Морзе **«Құпия хат-хабарларға арналған сөздік»; «Морзе электромагниттік телеграфында пайдалану үшін бейімделген». « Қауіпсіздікті қамтамасыз ету үшін телеграфтық байланыс»** желілерінде оңай енгізілген шифрлауды қолданатын кодты қолдану ұсынылды. Кейіннен шифрлауды дамыту және механикалық шифрлау құрылғыларын құру оларды телеграф байланысында қолдануды ескере отырып жүргізілді.

А.С.Поповтың радиосы

2. РАДИО

1895 жылы ресейлік ғалым **А.С.Поповтың** арқасында әлемге коммуникацияның жаңа тәсілі пайда болды - оның пайда болуы криптографияның дамуына үлкен әсер етті. Жіберілген хабарламалардың көлемін бірнеше есе ұлғайтуына байланысты (құпияларды қоса алғанда) ақпаратты қорғау үшін жаңа және жаңа кодтарды жасау қажет болды.

Қабырғаға орнатылған телефон аппараты Lars Mangus Ericsson, Стокгольмде дайындалған

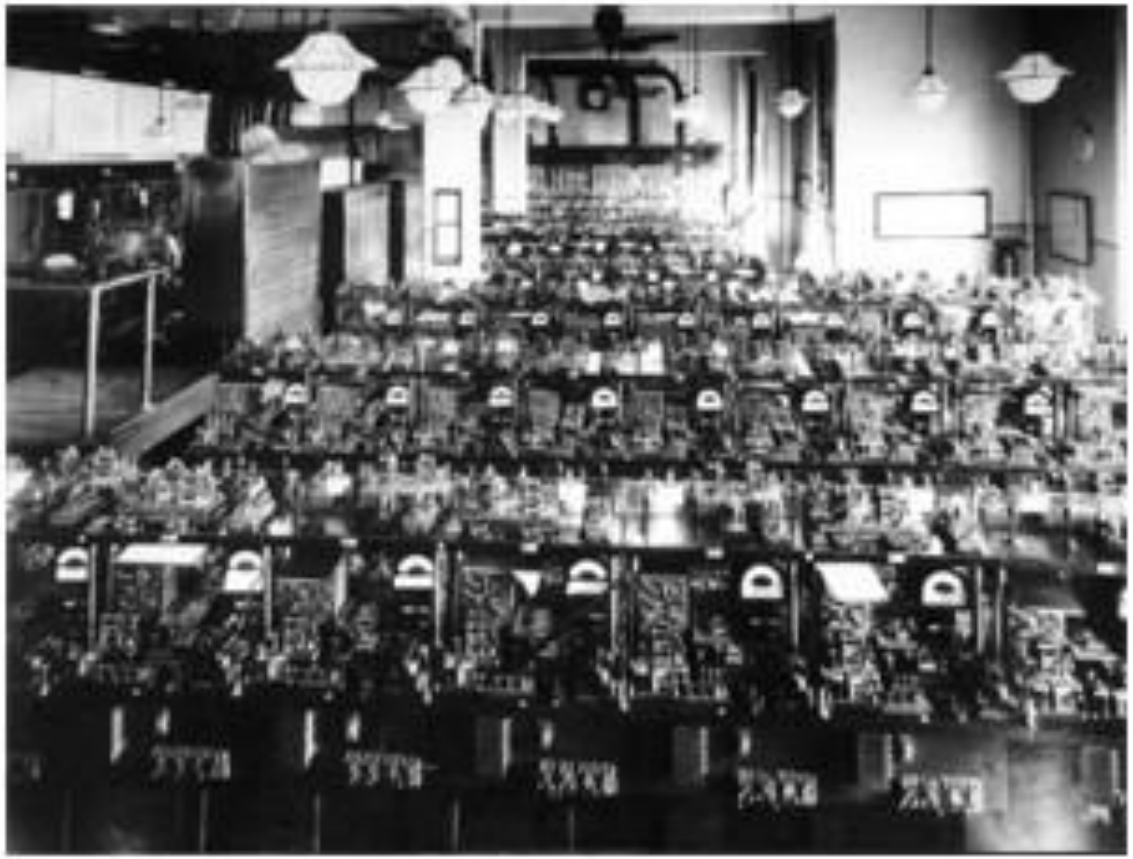
3.ТЕЛЕФОН

- 1876 жылы американдық А.Белл сымды телефонды ашық түрде көрсетті. Жақында жаңа өнертабыс әлемде кеңінен танымал болды, бірақ құпия ақпараттың телефон арқылы жіберілу проблемасы пайда болды.

- 5 жылдан кейін тағы бір американдық **Дж. Роджерс** келесі жолды ұсынды. Ол былай деп жазды: «Менің өнертабысым мынада, бұл хабар ... екі (немесе одан да көп) тізбектерге тез арада дәйекті импульстар арқылы жіберіледі ... сондықтан тізбектердің біреуіне ғана жалғасатын адам түсініксіз сигналдарды алады ...

Күрделі интерференциямен күресу үшін **«классикалық әдіс»** ұсынылды: әріптер қысқаша сөз түрінде берілді (көбіне аттар): А = Анна, Б = Борис және т.б.

XIX ғасырдағы криптографияның даму ерекшеліктері



Қорытынды

- Криптография «ашық әлемге» кірді. Оның әңгімелеріне сүйене отырып, өнер туындылары (**Эдгар По, Артур Конан Дойл**) белсенді түрде ойнай бастады. XX ғасырдың өзінде Д.Каун криптографияны **«царицей головоломок»** деп атады. Криптография дербес ғылыми пән ретінде бұрын онымен байланыспаған ғалымдардың назарын аудара бастады. Ол үкіметтік емес ұйымдармен және қылмыстық әлеммен белсенді пайдаланылды. Криптографиялық әдістер қолданыла бастады және тарихшылар **«умерших языков»** құпияларын ашумен айналысты.

Қолданылған әдебиеттер тізімі:

http://home.luna.nl, Виртуальный компьютерный музей
Литература:
Frost & Sullivan, “The Military Communications Market in the U.S.”, 1983.
Jane’s Military Communications 1966,…2000.
Kahn D. The codebreakers. N.-Y., 1967.

Бабаш А. В., Шанкин Г. П. История криптографии. Часть 1. М., “Гелиос”, 2002.
Вальдман Э. К. Занимательная телеграфия и телефония. М., “Связь”, 1964.
Жельников В. Криптография от папируса до компьютера. М., 1996.
Калачев К. В круге третьем. М: 1999.
Кукридж Е. Х. Тайны английской секретной службы. М., 1959.
Мазер И. Дипломаты и дипломатия // “За рубежом” № 17, 1993.
Найтли Ф. Шпионаж XX века. М., 1994.
Полмар Н., Аллен Т. Б. Энциклопедия шпионажа. М., 1999.
Саломаа А. Криптография с открытым ключом. М., 1997.
Соболева Т. А. Тайнопись в истории России. М., 1994.
Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.