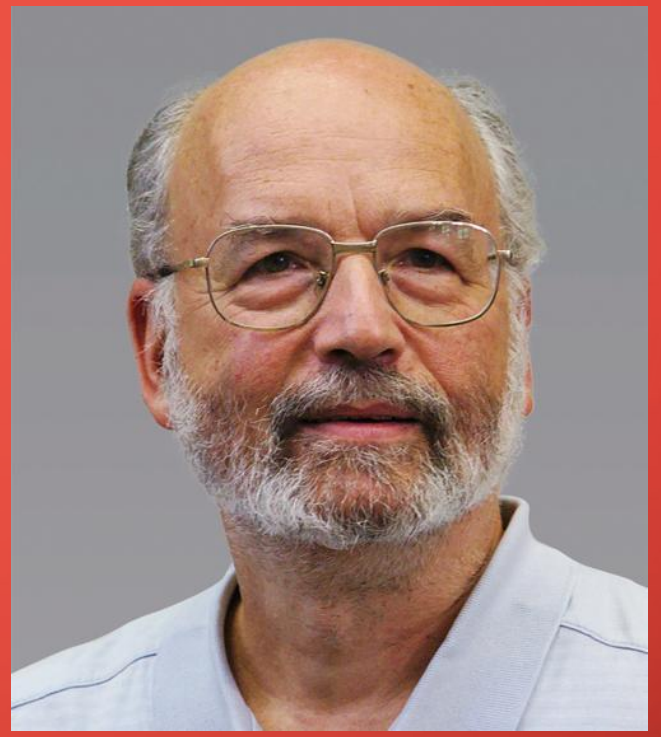
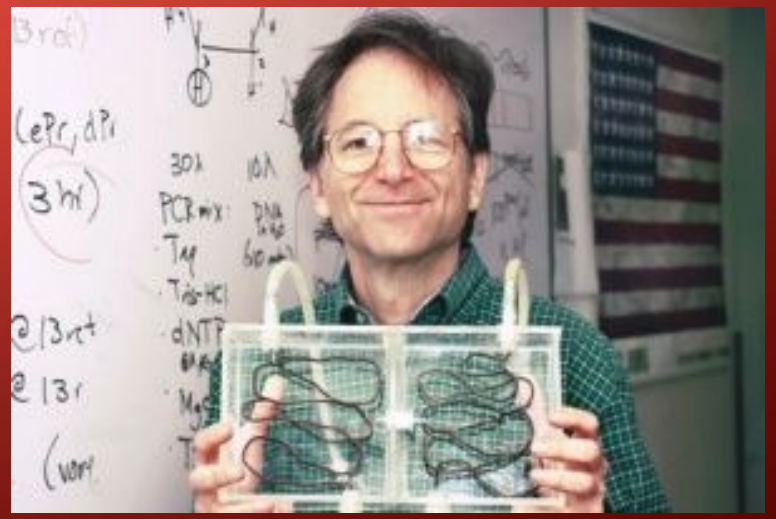
ЭЛЕКТРОНДЫ САНДЫҚ ҚОЛТАҢБА

- RSA криптожүйесін Рон Ривест (Ron Rivest), Ади Шамир (Adi Shamir) және Леонард Адлеман (Leonard Adleman) 1978 жылы ойлап тапқан. Алгоритм үлкен санды жай көбейткіштерге жіктеу есебінің қиындығына сүйенген. Алгоритмнің беріктілігі дискреттік логарифмді есептеудің қиындығы мен үлкен сандардың қиындығының мәніне негізделеді.





- RSA (1977 жыл) – ашық кілтті криптографиялық жүйе.
- Шифрлеу және цифрлік қол деген қорғау механизмдерін
- қамтамасыз етеді.
- RSA алгоритмі Internet-те қолданылады, мысалы:
- S/MIME
- • IPSEC (Internet protocol Security)
- • TLS (осымен SSL-ді алмастыруы мүмкін)
- • WAP WRLS
- RSA АЛГОРИТМІ
- • Ассимметриялық криптожүйе негіздеріне
- біржақты функциялар мен ілік-функцияларды
- құруға мүмкіндік беретін математиканың қиын
- мәселелерінің бірі қойылады.

- Электрондық сандық қолтаңба (ЭСҚ) – бұл электрондық құжаттың деректемесі, жасанды көшірмеден осы электрондық құжатты қорғау үшін арналған. Электрондық сандық қолтаңба ақпаратты криптографиялық қорғау құралдарын (АҚҚҚ) пайдалануымен ақпаратты қайта жасау нәтижесінде қалыптасады және кілттің қол қою сертификатының иесін сәйкестендіруге, сондай-ақ электрондық құжатта ақпараттың бұрмалануының жоқ болуын белгілеуге рұқсат етеді.

- Қолтаңбаны пайдалану өте қарапайым. Ешқандай аранайы білім, дағдылар және икемділік бұл үшін талап етілмейді. Электрондық құжаттарды алмасуға қатысушысы, электрондық сандық қолтаңба әрбір пайдаланушысына бірегей ашық және жабық (құпия) криптографикалық кілттер туындатады.[5]
- Негізгі элемент құпия кілт болып табылады, оның көмегімен электрондық құжаттардың шифрлеуі жасалады және электрондық сандық қолтаңба қалыптасады. Сонымен қатар құпия кілт пайдаланушыда қалады, оған бөлек тасығышта беріледі, бұл дискета, смарт-карта или touch memory болуы мүмкін. Оны басқадай пайдаланушылардың желісінен құпияда сақтау қажет.

Электрондық сандық қолтаңба түпнұсқасын тексеру үшін ашық кілт пайдаланылады. Куәландырушы орталығында ашық кілттің телнұсқасы тұр, ашық кілттердің тіркеу куәліктерінің кітапханасы құрылған. Куәландырушы орталық ашық кілттердің тіркеуін және бұрмалауды енгізуден немесе жасанды көшірмені жасаудан қашуға сенімді сақтауды қамтамасыз етеді.[6]

Сіз электрондық құжатқа тиістіге өзіңіздің электрондық сандық қолтаңбаңызды орнатасыз. Бұл ретте электрондық сандық қолтаңба құпия кілтінің және ұсталатын құжаттың негізінде криптографиялық қайта жасау жолымен кейбір үлкен сан қалыптасады, ол осы нақты құжатқа тиісті осы пайдаланушының электрондық сандық қолтаңбасы болып табылады. Электрондық құжаттың аяғына осы сан қосылады немесе бөлек файлда сақталады.

Қолтаңбаға мынадай ақпарат жазылады:

- Қолтаңба ашық кілті файлының аты.
- Қолтаңбаны қалыптастырған тұлға туралы ақпарат.
- Қолтаңбаның қалыптасқан күні.

- Жөнелтуші құжатының мәтіні және ашық кілтінің негізінде жөнелтушінің электрондық сандық қолтаңба ашық кілтіне ие және қол қойылған құжатты алушы, жөнелтушінің электрондық сандық қолтаңбасының тексеруін қамтамасыз етуші, кері криптографиялық қайта жасауды орындайды. Егер электрондық сандық қолтаңба құжатқа тиістісі дұрыс болса, онда яғни бұл құжат шынында жөнелтушімен қол қойылған және құжаттың мәтініне ешқандай өзгертулер енгізілмеген. Әйтпесе жөнелтушінің сертификаты шынайы болып табылмайды деп хабарлама берілетін болады.

Электрондық сандық қолтаңба – уақыттың жаңа талаптарымен бірге кім қадам басуды қалағандардың барлығы үшін тиімді шешім. Егер алынған ақпараттың келісім қортындысын немесе түпнұсқалығын растауды тексеру үшін жүздеген шақырымнан фельдъегерлік немесе шабармандық поштаның келуін күтуге уақытыңыз болмаса. Электрондық сандық қолтаңба артықшылығы анық - электрондық сандық қолтаңбамен қол қойылған құжат, бірнеше секундта белгіленген жеріне берілуі мүмкін. Құжатты электрондық алмасудың барлық қатысушылары олардың бір бірінен қашықтығына байланысты емес тең мүмкіншілікті алады. Шек жаңа технологиялардың арқасында 21 ғасырда жойылады.[10]

Электрондық сандық қолтаңба жасанды көшіру мүмкін емес – ол үшін есептеп шығарудың орасан санын талап етеді, ол қолайлы уақытта заманауи деңгейдегі есептеу техникасы мен математиканы іске асыру мүмкін емес, яғни қол қойылған құжатта ұсталатын әзірге ақпарат, өзектілікті сақтайды.

Жасанды көшірмеден қосымша қорғау қолтаңбаның ашық кілті куәландырушы орталығының сертификатымен қамтамасыз етіледі. Одан басқа клиенттің қалауы бойынша куәландырушы орталық клиенттің электрондық сандық қолтаңба сақтандыра алады.

Электрондық сандық қолтаңба пайдаланумен ойлау ауысады, "электрондық түрде жобаны әзірлеудің – қол қою үшін қағаз көшірмесін жасау – қол қойылуымен қағаз көшірмелерді жіберу - қағаз көшірмелерді қарау – оны электрондық түрде компьютерге көшіру" келмеске кетеді