Шифрлаудың симметриялы және ассиметриялы криптожүйесі. Электронды қолтаңба және хэштеу функциясы.

Криптография шифрлау жүйелерінің құруын және пайдалануын зерттейді, соның ішінде түрлі ашу әдістер жөнінде олардың беріктігін, осал жерін және осалдық дәрежесін.

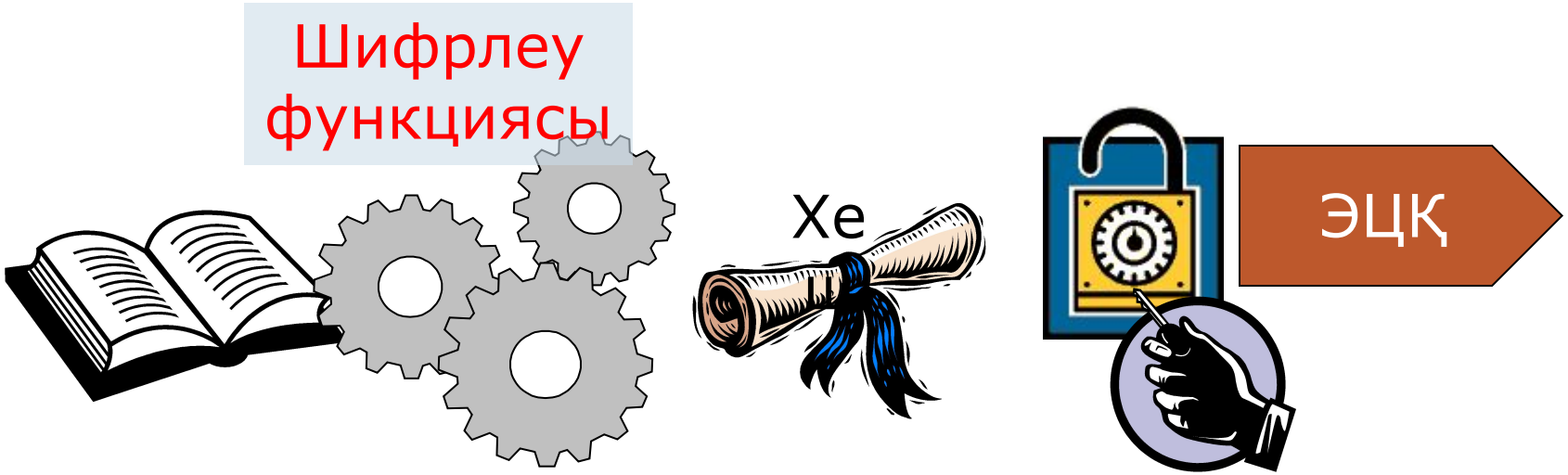
Шифрлау жүйесі немесе шифржүйесі – хабардың мәтінің қайтымды өзгерту үшін (жолданған адамнан басқа барлықтарға мәтін түсініксіз болсын оймен) пайдаланатын кез келген жүйе.

Шифр – бастапқы құпиялы хабарды қорғау үшін оның алдын ала айтылған түрлендіру тәсілдерінің жиынтығы.

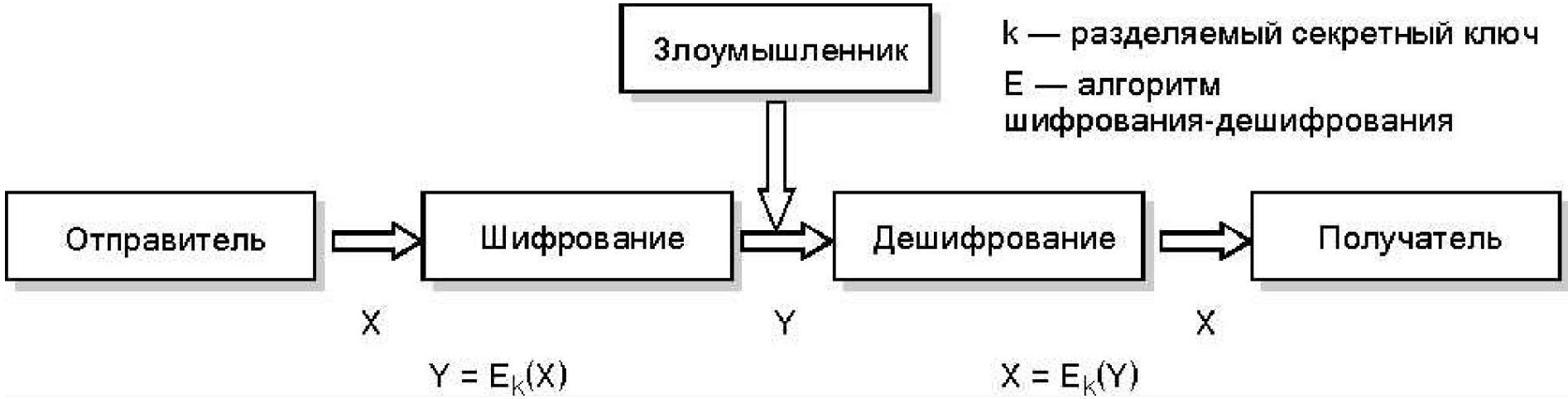
Симметриялық шифрлеу

Асимметриялық шифрлеу

Сандық қолтаңба



Симметриялық шифр

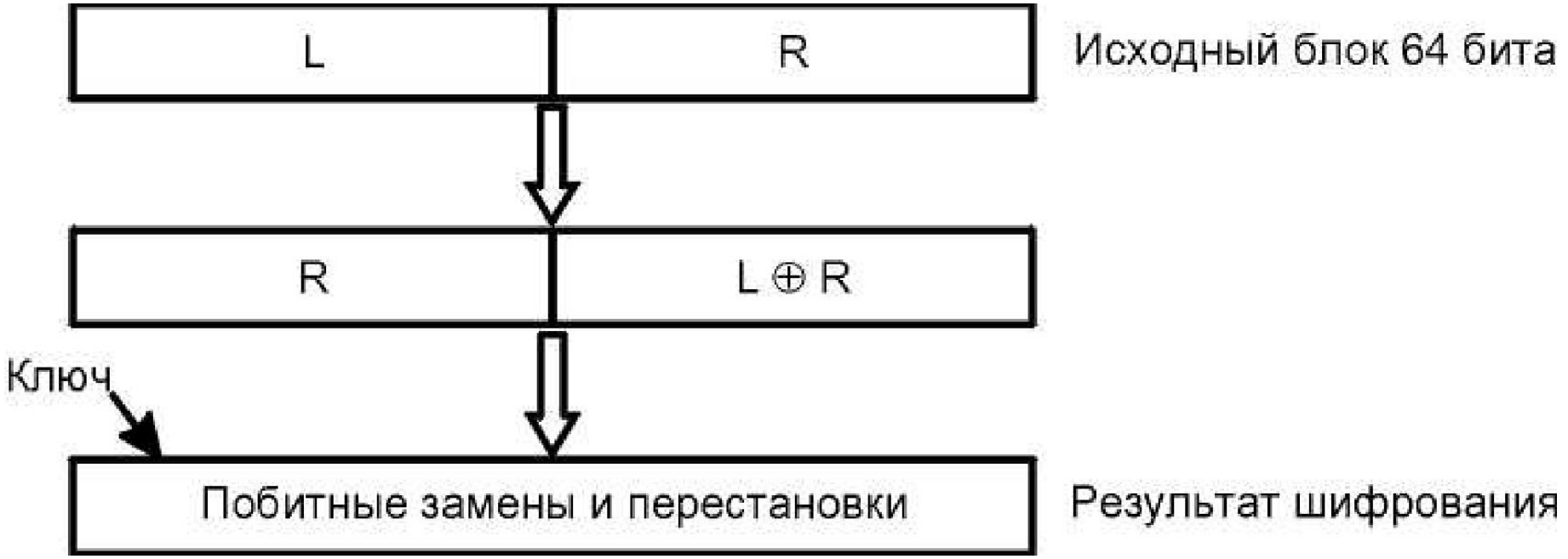


1949 жыл Клод Шеннон

DES алгоритмі бойынша шифрлау концепциясы

DES (Data Encryption Standard)

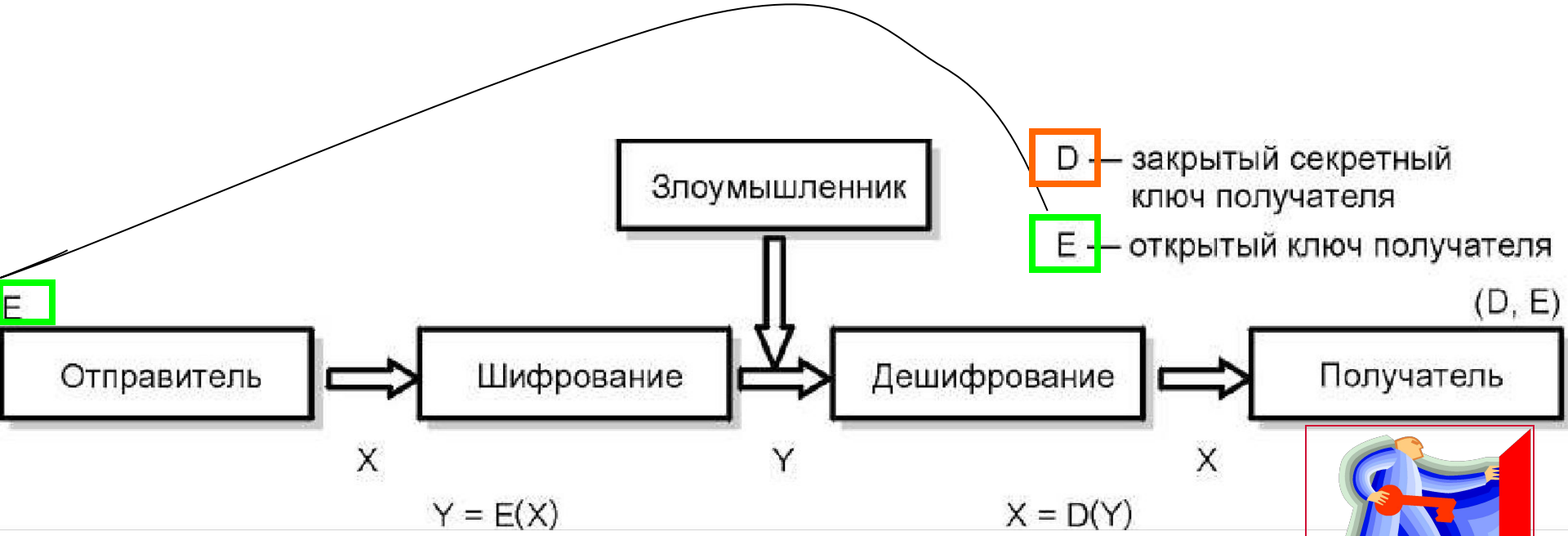
Алгоритм IBM фирмасымен 1976 жылы құрылған

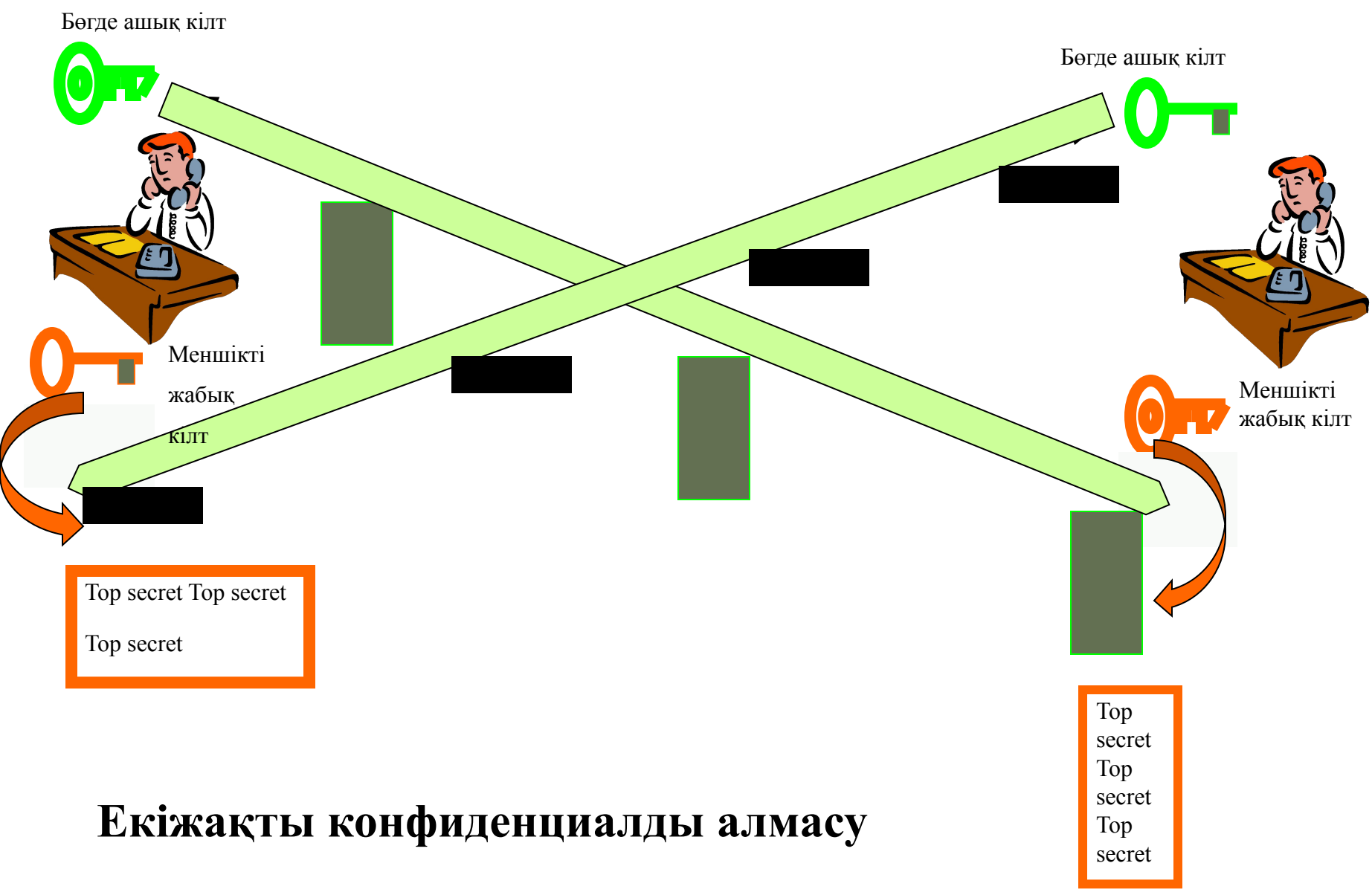


Triple DES (112 бит) – өнімділігі төмен

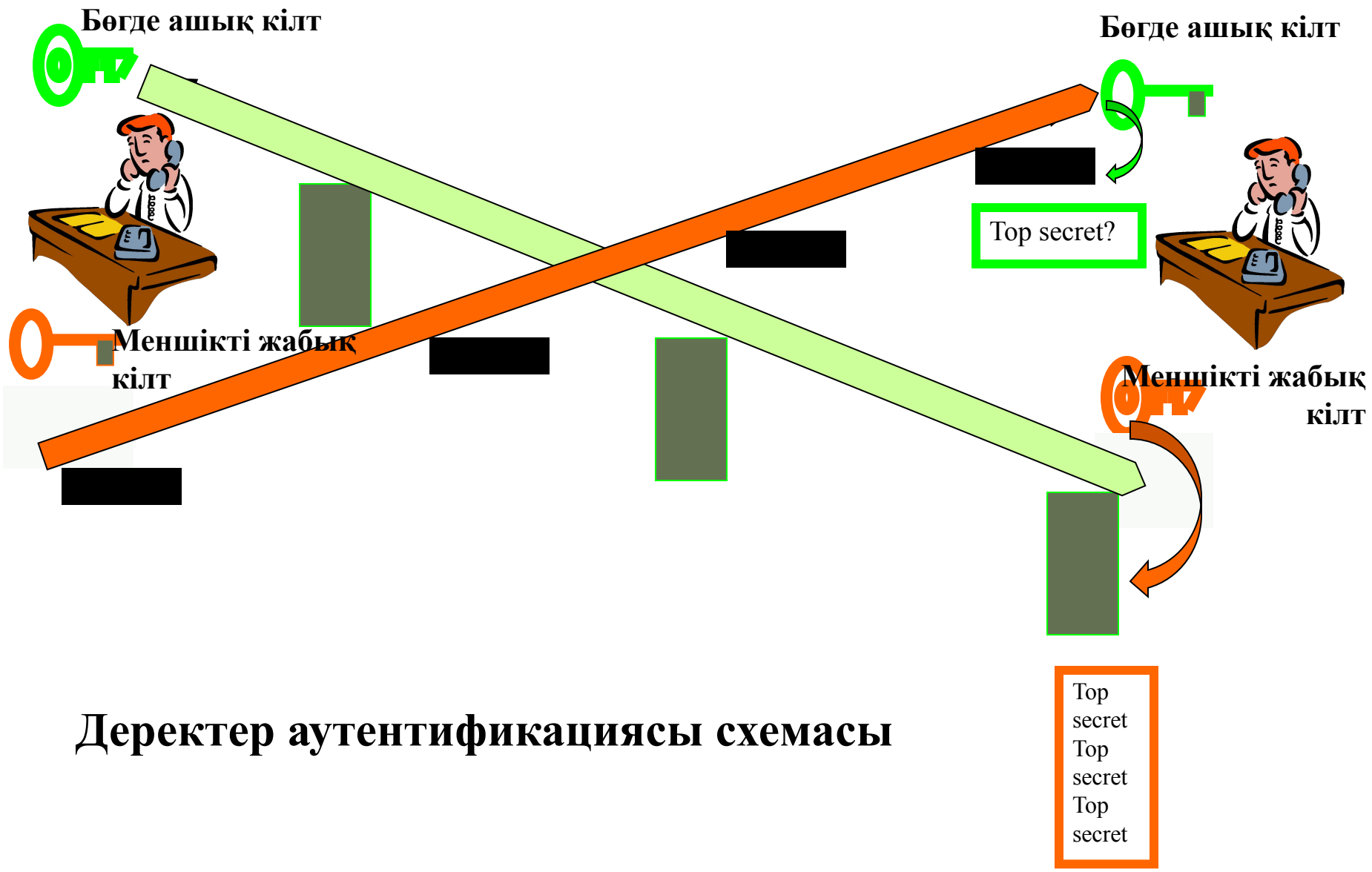
Ассимметриялық шифрлеу

70-жылдар ортасы —Диффи и Хеллман

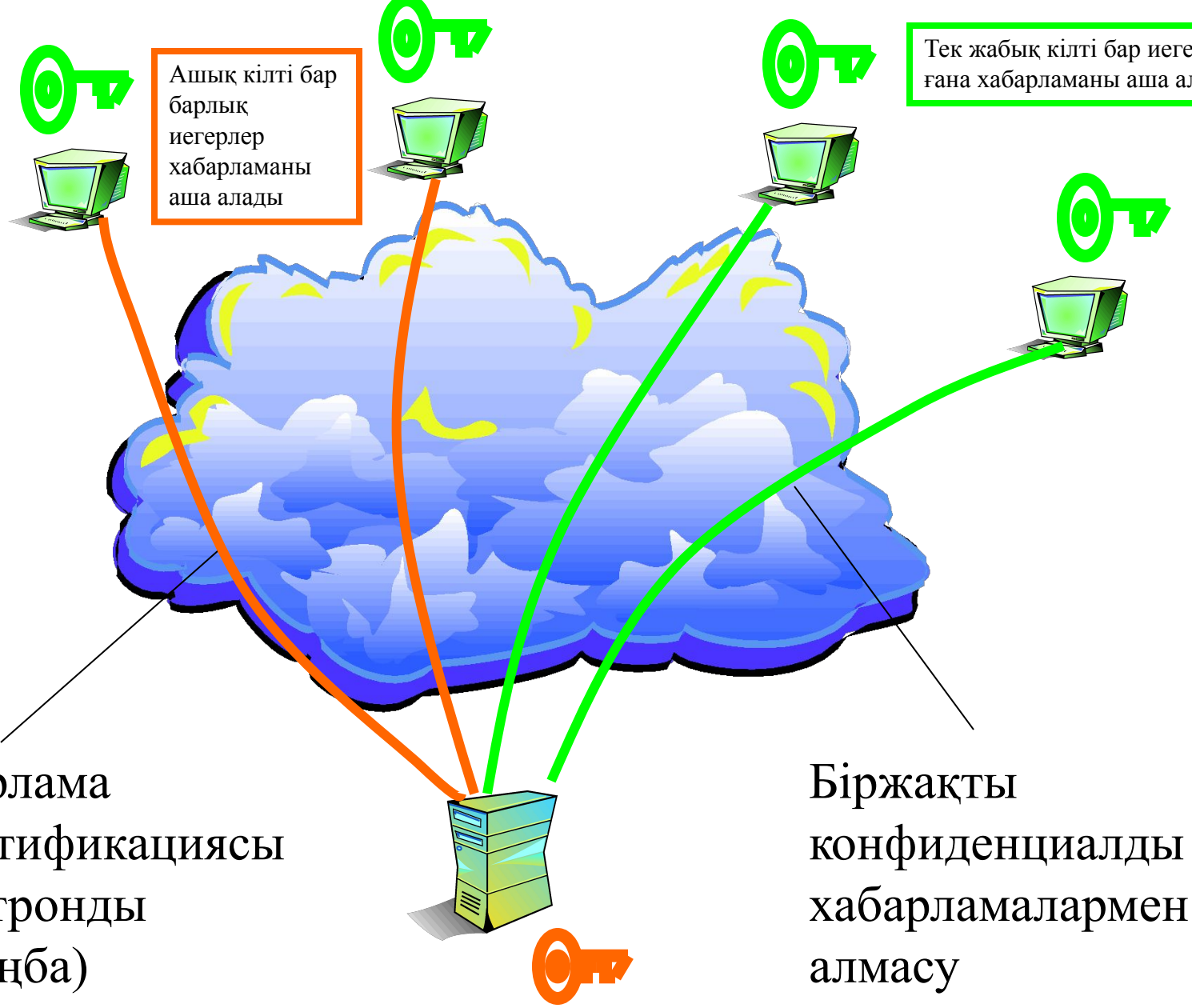




Екіжақты конфиденциалды алмасу схемасы



Деректер аутентификациясы схемасы



Хабарлама аутентификациясы (электронды қолтаңба)

Біржақты конфиденциалды хабарламалармен алмасу

Симметриялық және ассиметриялық шифрлауды қолдануды біріктіру

SKIP (Simple Key management for Internet Protocol) протоколы

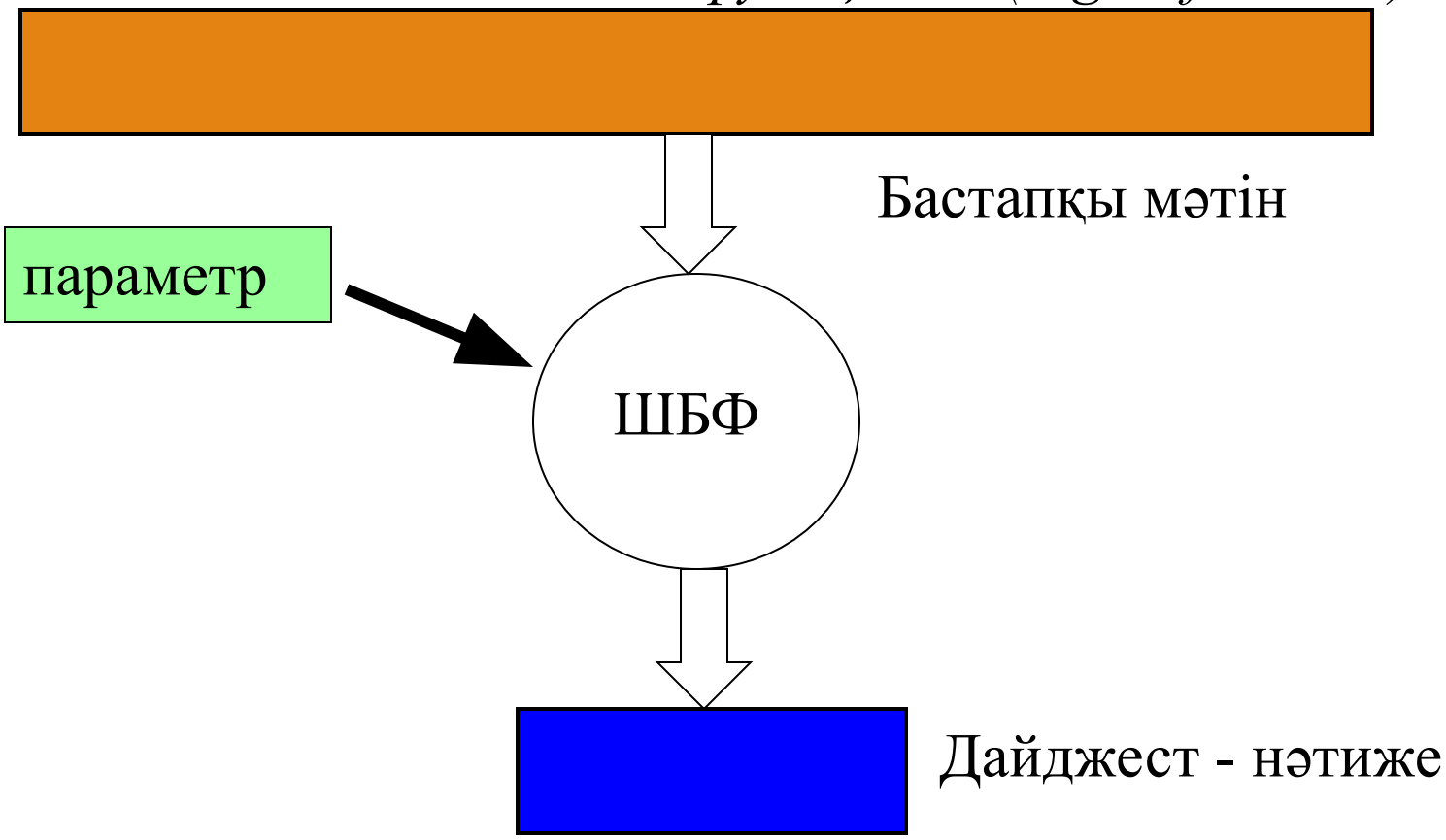
- IP-пакеттер симметриялық алгоритм негізінде шифрланады
- Шифрлау үшін кілт ассиметриялық алгоритмді қолдану арқылы есептеледі

Шифрлеудің біржақты функциялары

(ШБФ) (one-way function)

хэш-функциясы (hash function)

дайджест-функциясы (digest function)



Ең көп танымал хэш- функциялар:

- **MD2, MD4, MD5** – белгіленген 16 байт ұзындықты дайджесттер
- **SHA** – американдық стандарт, MD4 –тің бейімделген нұсқасы, дайджест ұзындығы 20 байт
- **MDC2, MDC4** - IBM компаниясы қолдайды

Шифрлеудің біржақты функцияларын тағайындау

(1) Тұтастылықты бақылау

(2) Шынайылықты бақылау