## 8 Зертханалық жұмыс №8. Кілттерді генерациялау үшін ақпараттық-бағдарламалық құралдарды пайдалану. E-mail-мен хабарлар алмасу кезінде ЭЦҚ-ны және шифрлауды қолдану

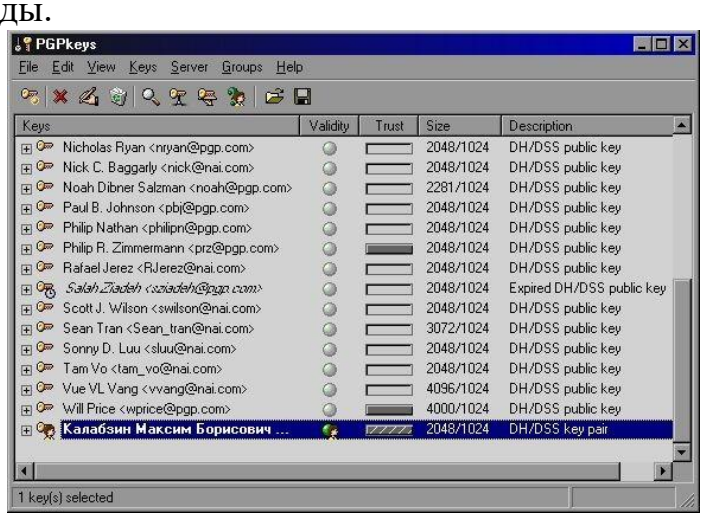
**Жұмыстың мақсаты:** e-mail бойынша хабарламалармен алмасу процесінде PGP бағдарламасымен жұмыс істеу мысалында электронды цифрлік қолтаңбаны (ЭЦҚ) қолдану принципін меңгеру.

### 8.1 Әдістемелік нұсқаулар

ЭЦҚ технологиясы көзқарасымен – бұл құжатты шифрлейтін және онымен қолтаңба сол немесе басқа электронды құжатта тұрғанын және оның қандайда бір басқа адаммен емес автормен қойылғандығын дәлелдеуге мүмкіндік беретін бағдарламалық-криптографиялық құрал [5].

Жұмыс топта орындалады: екі студент және оқытушы. Жұмысты орындау тізбегі «Тапсырма» бөлімінде сипатталған. Төменде жұмысты орындау реті сипатталған.

Жабық кілтті құру үшін кілттер – кілттер реестрімен жұмыс істеудің негізгі терезесін ашу керек. Оны "Пуск/Programs/P G P/PGPkeys" менюі арқылы істеуге болады.




8.1 сурет –PGPkeys бағдарлама интерфейсі

### 8.2 Жұмысты орындауға тапсырмалар

Жабық кілт құрыңыз. «Full name» жолында өз атыңыз бен тобыңызды пайдаланыңыз.

Жаңа ғана құрылған жабық кілтті пайдалана отырып, дискте ашық кілт құрыңыз.

Ашық кілтті оқытушыға электронды пошта арқылы жіберіңіз (ендірілген файл түрінде жіберуге болады). Оқытушының электронды поштасының адресі: prep@meit.stu.ru.

Сізге пошта арқылы оқытушының ашық кілті келгенін тосыңыз, оны

дискте сақтап, реестрге орнатыңыз.

MS Word редакторында құжат құрыңыз, мәтінде өз фамилияңызды көрсетіңіз. Құжат файлын латын әліпбиінің символдарымен атаңыз. Құжатқа өз суретіңізді қойыңыз. Файлды цифрлік қолтаңбамен қол қойыңыз, ол үшін өзіңіздің жабық кілтіңізбен оқытушының ашық кілтін қолданыңыз. Бұл файлды ендірілген түрде электронды пошта арқылы оқытушыға жіберіңіз.

Оқытушыдан зертханалық жұмыстың бірінші бөлімі тапсырылғандығы туралы хабарлама күтіңіз. Хатқа ендірілген файлды шифрден шешіңіз.

Бұл файлдың мазмұнын оқытушыға көрсетіңіз!

Осылайша топ студенттерінің бірімен ЭЦҚ қол қойылған файлдармен алмасуды жүзеге асырыңыз, ол үшін алдымен ашық кілттеріңізбен алмасыңыздар. Өзіңіздің ашық кілтіңізді алушыға жіберіп, алушыдан оның ашық кілтін күтіп, оны реестрге орнатыңыз.

MS Word дербес мазмұны бар ақпаратпен файл құрыңыз. Файлды өзіңіздің жабық кілтіңіз бен алушының ашық кілтін пайдалана отырып, цифрлік қолтаңбамен қол қойыңыз.

Бұл файлды алушыға жіберіңіз. Алушыдан ендірілген файлмен хатты күтіп, шифрден шешіңіз.

Бұл файлды оқытушыға көрсетіңіз!

Ескерту: Басқа студенттен хабарлама алу үшін сізге өзіңіздің Outlook Express бағдарламасы бапталған e-mail адресіңізді білу қажет. Ол үшін бағдарламады «Сервис / Учетные записи» меню пунктін таңдаңыз. Барлық есептік жазбалар тізімімен терезе ашылады. Мысалы келесі түрде жазба таңдап алынады: «10.242.48.45 пошта (үнсіз келісім бойынша)», нажмите «Свойства» батырмасын шертіңіз. Ашылған терезеден пошталық аккаунттың барлық баптауларын көруге және қажет кезде оларды өзгертуге болады.

**Бақылау сұрақтары**

1. ЭЦҚ нені көрсетеді?
2. Ашық және жабық кілттер немен ерекшеленеді?
3. Цифрлік қолтаңбамен хабарламаны қалай шифрлеуге болады?
4. Алынған хабармаланы қалай шифрден шешуге болады?
5. ЭЦҚ жұмыс істеу үшін қандай бағдарламалық өнімдер қолданылады?
6. ЭЦҚ дегеніміз не?
7. ЭЦҚ жұмыс істеу принципі.
8. Кілттер не үшін қажет?