**RSA АЛГОРИТМЫ**

**Кіріспе**

**RSA (Rivest-Shamir-Adleman) –** ашық кілтті криптографиялық алгоритм.

Ол 1977 жылы Рон Ривест, Ади Шамир және Леонард Адлеман тарапынан жасалды. RSA алгоритмі сандардың үлкен көбейткіштерге жіктелуінің күрделілігіне негізделген. Ол екі кілтті қолданады:

* **Ашық кілт (public key)** – шифрлау үшін қолданылады және оны барлығы біле алады.
* **Жабық кілт (private key)** – тек иесіне белгілі және шифрланған ақпаратты шешу үшін қолданылады.

Бұл жерде біз RSA алгоритмінің жұмысын Python тілінде іске асырамыз. Берілген параметрлер:

* p = 7
* q = 13
* e = 5
* M = 12

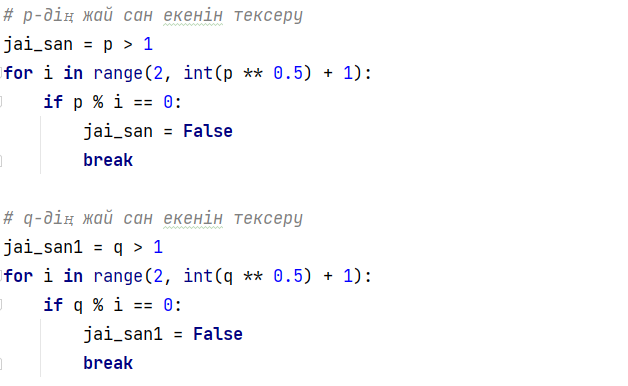
1. **Бастапқы параметрлерді орнату**

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

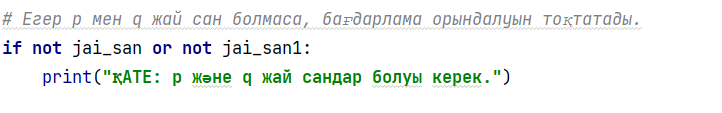
* Бұл жерде M – шифрланатын сан, ал p және q – екі үлкен жай сан.

**2. p және q сандарының жай екенін тексеру**



* Мұнда **жай санды тексеру** үшін **p және q** сандарының **1-ден үлкен** екенін және басқа сандарға бөлінбейтінін анықтаймыз.

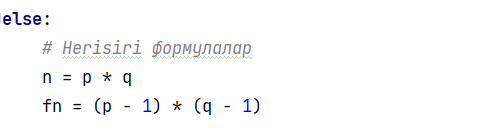
**3. Егер p мен q жай сан болмаса, бағдарламаны тоқтату**



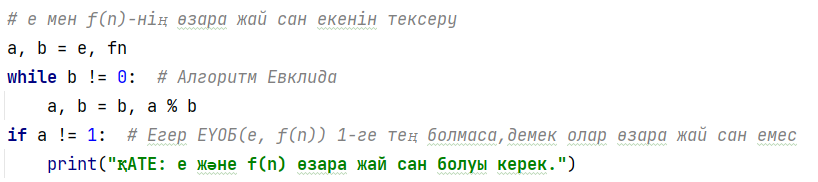
* Егер **p немесе q** жай сан болмаса, бағдарлама орындалмайды.

**4. Егер жай сан болса ары қарай жалғастыру**

**Негізгі формулалар 🡪 n = p \* q және φ(n) = (p-1) \* (q-1) мәндерін есептейміз.**

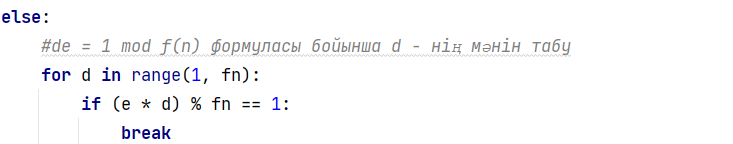
****

**5. e және φ(n) өзара жай сандар екенін тексеру**

****

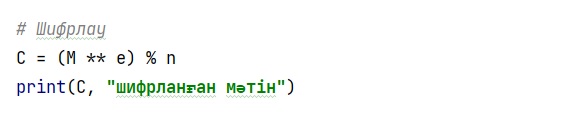
* Бұл жерде Евклид алгоритмі арқылы e және φ(n) сандарының өзара жай екенін тексереміз.

**6. Жабық кілтті (d) табу**

****

* d мәні (e × d) mod φ(n) = 1 шартын қанағаттандыратын ең кіші сан ретінде табылады.

**7. Шифрлау процесі және нәтижені алу**



**НӘТИЖЕ:**

****

**M мәтінін C = Me mod n формуласы бойынша шифрлаймыз.**

**5. ҚОРЫТЫНДЫ**

RSA алгоритмі  **ассимметриялық криптография** әдістерінің бірі болып табылады. Бұл әдіс **p және q** жай сандарын пайдаланып, **ашық және жабық кілттерді** есептеуге негізделген. Шифрлау **C = Me mod n** формуласымен, ал кері шифрлау **M = Cd mod n** формуласы арқылы жүзеге асады.

Бұл алгоритм кеңінен қолданылады және **берілген кілттер ұзындығына** байланысты қауіпсіздік деңгейі жоғары болып саналады.

**ПРАКТИКАЛЫҚ ТАПСЫРМАЛАР**

**1-тапсырма: Берілген параметр:**

* p = 11, q = 17
* e = 7
* Мәтін: M = 8

**Шифрмәтінді (C) табыңыз.**

**2-тапсырма: Дешифрлау**

Мысалдағы 38 шифрланған мәтінін дешифрлайтын бағдарлама құрыңыз.

**3-тапсырма: Шифрлау**

" **CRYPTO** " сөзін шифрлаңыз.( " **CRYPTO** " мәтінін ASCII кодына түрлендіріңіз)

Параметрлер:

* p=17
* q=19
* e = 13