**ГАММАЛАУ АРҚЫЛЫ ШИФРЛАУ**

**(ЕКІЛІК МОДУЛЬ, UTF-8)**

**Кіріспе**

**Гаммалау әдісі** – симметриялық шифрлау әдістерінің бірі, онда ашық мәтін кілт (гамма) көмегімен XOR (екілік модуль бойынша қосу) операциясы арқылы шифрланады. Бұл әдістің басты ерекшелігі – бастапқы мәтінді қалпына келтіру үшін дәл сол гамманы пайдалану керек.

Бұл жерде біз **Kazakhstan** сөзін **Astana** гаммасымен UTF-8 кодтауында шифрлаймыз.

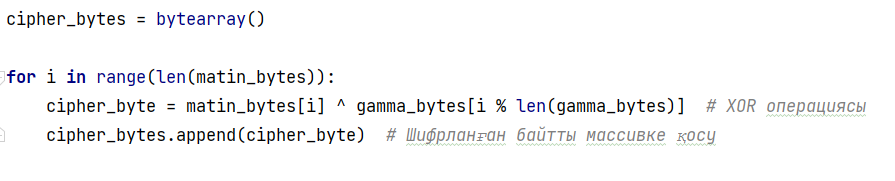
**1. Ашық мәтінді және гамманы дайындау**

* Бұл жерде **Kazakhstan** және **Astana** сөздерін UTF-8 кодтауында байттарға айналдырдық.

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

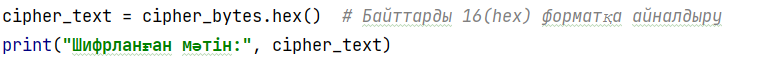
**2. Гаммалау әдісімен шифрлау**



**Түсініктеме:**

* Әрбір байтты гаммадағы сәйкес байтпен XOR (^) операциясы арқылы шифрлаймыз.
* Егер гамманың ұзындығы мәтіннен қысқа болса, оны қайталаймыз (i % len(gamma\_bytes) арқылы).
* Шифрланған нәтижені cipher\_bytes массивінде сақтаймыз.

**3. Шифрланған мәтінді шығару**



Шифрлау нәтижесі: **"0A 12 0E 00 05 09 32 07 15 0F" .**Бұл HEX түріндегі шифрланған мәлімет**.**



**4. ҚОРЫТЫНДЫ**

* Бұл жерде біз Kazakhstan сөзін Astana гаммасымен XOR операциясы арқылы шифрладық.
* UTF-8 кодтауы қолданылды, сондықтан кез келген символдарды шифрлауға болады.
* Шифрланған нәтиже HEX форматында сақталды.

**Гаммалау әдісі** – заманауи криптографияның негізі болып табылады, алайда кілттің кездейсоқ болуын және қайта қолданылмауын қамтамасыз ету маңызды.

**ПРАКТИКАЛЫҚ ТАПСЫРМАЛАР**

**1-тапсырма: Шифрлау**

Өз есімінізді XOR әдісін қолданып шифрлаңыз.

* **ГАММА - Тегіңіз**

**2-тапсырма: Дешифрлау**

Мысалдағы " **0A 12 0E 00 05 09 32 07 15 0F** " шифрланған мәтінін дешифрлайтын бағдарлама құрыңыз.

**3-тапсырма: Шифрлауды анықтау**

" **КРИПТОГРАФИЯ** " сөзін шифрлаңыз.

* **ГАММА – “АЛГОРИТМ”**