Лекция 10 АШЫҚ КІЛТІ БАР КРИПТОГРАФИЯДА ПАЙДАЛАНАТЫН САНДАР ТЕОРИЯСЫНЫҢ НЕГІЗГІ ҚАҒИДАЛАРЫ

1 Жай және құрама сандар

Әрбір бірден үлкен натурал сан ең азы екі санға бөлінеді: 1-ге және өз өзіне. Егер санның өзінен және бірден басқа бөлгіші болмаса, оны **жай сан** деп атайды, ал егер санда тағы бөлгіштері болса, онда **құрама** деп атайды. Бірді не жай не құрама деп атамайды. Мысалы, 7, 29 сандар — жай; 9, 15 сандар — құрама (тоғыз 3-ке бөлінеді, он бес 3 пен 5-ке бөлінеді).

Қызықты факт: егер екі жай сандардың айырмашылығы 2-ге тең болса, онда оларды «егіз»-сандар деп атайды. «Егіз»-сандар аса көп емес. Мысалы, 5 пен 7, 29 бен 31, 149 бен 151 «егіздер», және де $242\,206\,083 * 2^{38\,880} \pm 1$ (қазіргі уақытқа дейін табылған ең үлкен «егіз» жұбы).

Сан жай ма немесе құрама ма - тұра айту оңай емес. Егер сан жүзден кем болса, осындай сұраққа жауапты табу қиын емес. Бірақ үлкен сандарды анықтау күрделілен болады. Мысалы, 2009 санды алайық. Ол жай немесе құрама ма? Осы санның мүмкін бөлгіштерін алғашқы жай сандар арасынан іздеп табайық. 2009 әрине 2-ге бөлінбейді (өйткені ол тақ), 3-ке бөлінбейді (өйткені оның цифрлер қосындысы 2+9=11 3-ке бөлінбейді), 5-ке де бөлінбейді. Ал 2009-ды 7-ге бөлетін болсақ, нәтижесінде – 287 аламыз. Сонымен, жауап: 2009 саны – құрама. Мұнда жауап тез табылды. Бірақ, өте үлкен бүтін сандарды жайлыққа тексеру көп уақыт алады, және ол үшін арнайы компьютерлік программалар пайдаланады.

Үлкен жай сандарды іздеу математикадан басқа криптографияға да өте маңызды, олар ашық кілті бар шифрлау алгоритмдарда пайдаланылады. Шифрлаудың сенімділігін қамтамасыз ету үшін онда ұзындығы 1024 битке дейін жай сандар пайдаланады.

Екі санды көбейту қиын емес, әсіресе калькулятор бар болғанда және сандар аса үлкен болмаса. Кері есеп те бар – *факторизациялау есебі* – көбейткенде берілген санды беретін екі не одан көп санды табу. Бұл есеп көбейтуден өте күрделі. Мысалы, егер бізге 67-ң 113-ке көбейтуі керек болса, онда нәтижесін 7571 бір минуттан тез табуға болады. Ал егер бізге көбейтіндісі 7571-ге тең екі санды тап десе, оған анағұрлым көп уақыт кетеді.

n санның көбейткіштерін іздестіруін $\sqrt{n}$-ге дейін барлық жай сандарды іріктеп алып жүргізуге болады, мысалы 2009 сан сияқты. Бірақ, егер көбейткіштер – үлкен жай сандар болса, онда оларды іздеуге көп уақыт кетеді.

Сонымен, үлкен санды факторизациялау едәуір уақыт қажет етеді (бұл сан екі үлкен жай сандардың көбейтіндісі белгілі болғанда да).

Факторизациялау есебінің күрделілігі кейбір криптографиялық алгоритмда пайдаланылады, мысалы, RSA шифрлау жүйесінде.

10.2 Арифметиканың негізгі теоремасы

Кез келген құрама санды көбейту көмегімен кейбір жай сандардан құрастыруға болады. Мысалы, 2009 құрама санды былай табуға болады:

$$2009 = 7 \cdot 7 \cdot 41$$

Математикада **арифметиканың негізгі теоремасы** қарастырылады, ол бойынша кез келген натурал сан ($n>1$) не өзі жай болады, не жай бөлгіштердің көбейтіндісіне жалғыз ғана тәсілмен жіктелу мүмкін (көбейткіштердің жол ретін еске алмағанда).

Дәреже белгіні қолданып 2009 санды жай көбейткіштерге жіктелуі былай жазылады:

$$2009 = 7^2 \cdot 41$$

Көбейткіштерге жіктеу **канондық** деп аталады, егер барлық көбейткіштер жай болып өсу ретінде жазылатын болса.

Мысалы, 150 санның көбейткіштерге канондық жіктелуін жазайық:

$$150 = 2 \cdot 3 \cdot 5^2$$

10.3 Өзара жай сандар және Эйлер функциясы

Екі сан **өзара жай** деп аталады, егер олардың бірден басқа ешқандай ортақ бөлгіші болмаса.

Мысалы, 11 мен 12 сандар өзара жай (оларда бірден басқа ортақ бөлгіші жоқ), 30 және 35 сандар — өзара жай емес (оларда ортақ бөлгіші 5 бар).

Бүтін сандармен байланысты заңдылықтарды көп зерттеген болатын швейцар математигі Леонард Эйлер (Leonard Euler). Олардың арасындығы: *n*-ды аспайтын және *n*-мен өзара жай болатын қанша натурал сандар бар? Бұл сұраққа жауапты Эйлер 1763 жылы тапты және осы жауап *n* санның жай көбейткіштерге канондық жіктелуіне байланысты.

Егер

$$n = p_1^{a1} \cdot p_2^{a2} \cdot \ldots \cdot p_n^{an},$$

мұндағы $p_1, p_2, \ldots, p_n$ – әртүрлі жай көбейткіштер,

болса, онда *n*-нан аспайтын және *n*-мен өзара жай болатын натурал сандарды былай табуға болады:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$$

n-нан аспайтын және *n*-мен өзара жай болатын натурал сандардың саны **Эйлер функциясы** деп аталады және белгіленеді $\varphi(n)$.

Мысалы, 12-ден аспайтын және 12-мен өзара жай болатын натурал сандар саның табайық. Натурал сан қатарынан

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

12-мен өзара жай болатын тек 1, 5, 7, 11 сандар. Олардың саны төртке тең. Сонымен $\varphi(12)=4$.

Енді ($\varphi 2$) Эйлер формуласы бойынша есептеп көрейік. Ол үшін алдымен 12 санның канондық жіктеуін жазамыз:

$$12 = 2^2 * 3.$$

Эйлер функциясын $\varphi(12)$ есептейік:

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4 \cdot 3\frac{1}{2} \cdot \frac{2}{3} = 4.$$

Өзара жай сандарды қарапайым іріктеп алудан және Эйлер формула бойынша есептелген мәндер сәйкес келеді.

Эйлер формуласын үлкен n үшін пайдалану ыңғайлы, егер n санның жай көбейткіштеріне жіктеуі белгілі болса. Криптографияда Эйлер формуласының маңыздылығы – жай және кейбір басқа сандар үшін $\varphi(n)$ санды оңай табу мүмкіндігі. Криптографияда Эйлер формуласының келесі екі салдары пайдаланылады.

1-ші салдары. Егер p – жай сан, онда $\varphi(p) = p - 1$.

Шынында, егер p – жай сан, онда оның канондық жіктеуі тек өзінен ғана тұрады. Сонда

$$\varphi(p) = p \cdot \left(1 - \frac{1}{p}\right) = \frac{p(p-1)}{p} = p - 1.$$

2-ші салдары. p мен q — екі әртүрлі ($p \neq q$) жай сан болсын. Онда

$$\varphi(p \cdot q) = (p - 1)(q - 1).$$

Бұл формула келесі түрде түсіндіріледі. $p\ q = N$, мұнда p мен q — екі әртүрлі ($p\ q$) жай сан болсын. Сонда

$$\varphi(p \cdot q) = \varphi(N) = N \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = \frac{p \cdot q \cdot (p-1) \cdot (q-1)}{p \cdot q} = (p-1) \cdot (q-1).$$

Эйлер формуласы пайдалануының бірнеше мысалдарын қарап шығайық.

Мысал 1. $\varphi(13)$ табайық. 13 – жай сан, сондықтан, 1-ші салдарды пайдаланып $\varphi(13) = 13\text{-}1 = 12$. Өзімізді (және Эйлерді) тексерейік, ол үшін 13-тен кем барлық сандарды жазып:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,

12 олармен өзара жай барлық сандарды санайық. Шынында олар 12.

Мысал 2. $\varphi(35)$ табайық. 35 – құрама сан, демек бірінші салдары бізге келмейді. Бірақ 35 екі жай санның көбейтіндісі: $35 = 5\ 7$. 2-ші салдарды пайдаланып, есептейміз $\varphi(35)$:

$$\varphi(35) = (5\text{-}1)\cdot(7\text{-}1) = 4 \cdot 6 = 24.$$

35 тен кем және онымен ортақ бөлгіштері жоқ барлық сандарды жазып тексереміз:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

Шынында олардың саны 24.

Соңғы мысалдан көрініп тұр – көп сандарды қарастырғанша, Эйлер формуласын пайдалану ыңғайлы.

10.4 Қалдықтар арифметикасы және салыстыру теориясы

Неміс математигі Карл Фридрих Гаусс екі a мен b саны үшін

$$a \equiv b \pmod{m}$$

жазуды ұсынған болатын, егер оларда m-ға бөлуден бірдей қалдықтары бар болса (a модулі m бойынша b-мен салыстырлу деп оқылады). Мысалы,

$$\equiv \quad 1997 \quad 1 \pmod 4,$$

$7k + \equiv 1 \pmod 7$, мұндағы k – кез келген бүтін сан.

Салыстыруларда математиктар мен криптографтарға пайдалы қасиеттер бар, олар көбінесе теңдіктер қасиеттеріне ұқсайды. Бұл қасиеттер арифметикалық есептеулерді тым оңайлатады, егер бізге тек кейбір m санға бөлудің қалдығы керек болса. Мысалы, салыстыру қасиеттер ашық кілті бар шифрлау алгоритмдағы есептеуде пайдалы.

Салыстырулардың қарапайым қасиеттері келесі.

1-ші қасиет. Егер a-b m-ға бөлінсе, онда $a \equiv b \pmod{m}$.

Мысалы, $15 \equiv 1 \pmod 7$, өйткені 15-1 = 14, ал 14 7-ге еселі.

2-ші қасиет. Егер

$$a \equiv b \pmod{m}$$

және

$$c \equiv d \pmod{m}$$

онда

$$a + c \equiv b + d \pmod{m}$$
$$ac \equiv bd \pmod{m}.$$

Мысалы, $13 \equiv 5 \pmod 8$ және $11 \equiv 3 \pmod 8$ болғандықтан, онда $13+11 \equiv 5+3 \equiv 0 \pmod m$, және де $13 \cdot 11 \equiv 5 \cdot 3 \equiv 7 \pmod m$.

3-ші қасиет. Егер

$$a \equiv b \pmod{m}$$

онда

$$a^k \equiv b^k \pmod{m},\ k \subset N.$$

Мысалы, $25 \equiv 4 \pmod 7$ болғандықтан, онда $5^2 \equiv 2^2 \pmod 7$.

4-ші қасиет. Егер

$$ac \equiv bc \pmod{m}$$

және c m-мен өзара жай болса,
онда

$$a \equiv b \pmod{m}.$$

Мысалы, $1200 \equiv 45 \pmod 7$ белгілі, ал $1200 = 15 \cdot 80$ және $45 = 15 \cdot 3$, онда

$$80 \equiv 3 \pmod 7.$$

5-ші қасиет. Егер

$$ac \equiv bc \pmod{mc}$$

онда

$$a \equiv b \pmod{m}.$$

Мысалы, егер $44 \equiv 4 \pmod{4(10)}$ онда $11 \equiv 1 \pmod{10}$.

10.5 Ферманың кіші теоремасы

RSA жүйесі бойынша шифрлау алгоритмның негізінде XVII ғасырдың басында француз математигі Пьер Ферма (Pierre Fermat) тұжырымдаған теорема жатыр. Оны «Ферманың кіші теоремасы» деп жиі атайды, және танымал «Ферманың ұлы теоремасы» мен шатастырмау керек. Оны да ол дәлелдемей тұжырымдаған болатын, ал дәлелденген тек 1993-94 жылдары. Леонард Эйлер 1760 жылы Ферманың кіші теоремасын дәлелдеп, оның Ферма-Эйлер теоремасы деп аталатын жалпылауын тапқан болатын. Дәл осы теорема шифрлау/дешифрлау RSA алгоритмда пайдаланады.

Ферманың кіші теоремасы келесі түрде тұжырымдалады. Егер p – жай сан, ал m – p-ға бөлінбейтін кез келген сан болса, онда

$$m^{p-1} \equiv 1 \pmod{p},$$

яғни m^{p-1} саны p-ға бөлінгенде қалдықта 1 береді.

Мысалы, p=11, m = 3 болсын. 3^{10} mod 11 біргі тең болама тексерейік:

$$3^{10} \bmod 11 = 3^{2}(((3^{2})^{2})^{2}) \bmod 11 = 9(4^{2}) \bmod 11 = 144 \bmod 11 = 1$$

Эйлер тұжырымдаған және дәлелдеген жалпылау кез келген модуль үшін әділетті, бірақ RSA жүйеде дербес жағдайы пайдаланылады – онда модуль тек екі түрлі жай сандарының көбейтінідісі болып табылады. Сондықтан осы жағдайы үшін теореманың тұжырымдамасын қарастырайық.

Ферма-Эйлер теоремасы (RSA жүйенің жағдайы үшін). Егер p мен q – екі түрлі жай сандар, ал m – p мен q-ға бөлінбейтің кез келген сан болса, онда

$$m^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Мысалы, p = 11, q = 5 (pq = 55), m = 3 болсын. $3^{40} \equiv 1 \pmod{55}$ біргі тең болатының тексерейік:

$$3^{40} \bmod 55 = (3^{5})^{4} \bmod 55 = 23^{4} \bmod 55 = 279841 \bmod 55 = 1.$$

10.6 Ең үлкен ортақ бөлгіш

а мен *b* — екі бүтін оң сандар болсын. *a* мен *b* сандардың ең үлкен ортақ бөлгіші - бұл *a*-ны да *b*-ны да бөлетін ең үлкен *c* саны:

$$c = \text{ЕҮОБ}(a, b).$$

Мысалы, ЕҮОБ(25,35) = 5.

Ең үлкен ортақ бөлгішті табу үшін келесі, **Евклид алгоритмы** деп аталатын, алгоритмды пайдалануға болады.

```
Алгоритм NOD(бүтін a, b, c);
Басы
   1. a<>b болғанша орындау керек:
         1.1. Егер a>b онда a:=a-b, әйтпесе b:=b-a;
   2. c:=a;
Соңы.
```

Алгоритм орындалғаннан кейін нәтижесі *c* айнымалының ішінде болады.

Евклид алгоритмы көмегімен ЕҮОБ(18,9) есептеп көрейік:

```
a:     18   9
b:      9   9
c:      9   9
```

Мұнда әрбір баған алгоритмның кезекті итерациясы болып табылады. Процесс жүргізіледі *b* *a*-ға тең болғанша. Сонда *c* айнымалыға жауап жазылады, біздің жағдайда 9. Дәл осы ЕҮОБ(18,9)-ң мәні.

10.7 Евклидтың жалпыланған алгоритмы

Көптеген криптографиялық жүйелер үшін Евклидтың жалпыланған алгоритмы актуальды, онымен келесі теорема байланысады.

Теорема. *a* мен *b* — екі бүтін оң сандар болсын. Сонда *x* пен *y* бүтін (оң емес те болу мүмкін) сандар бар болады, олар үшін

$$ax + by = \text{ЕҮОБ}(a,b).$$

Евклидтың жалпыланған алгоритмы ЕҮОБ(*a*, *b*)-ны және жоғары жазылған теңдеуге сай келетін *x*, *y* іздеп табу үшін қызмет етеді. Үш жол енгізейік $U = (u_1,u_2,u_3)$, $V = (v_1,v_2,v_3)$ және $T = (t_1,t_2,t_3)$.

Алгоритм келесі түрде жазылады (кіру параметрде шарт *a≥b* орындалу керек).

```
Алгоритм ЕЖА(бүтін a, b);
Басы
  1. U = (a,1,0), V = (b,0,1).
  2.v1 <> 0 болғанша орындау керек:
    2.1. q = u1 div v1;
    2.2. T =(u1 mod v1, u2-qv2, u3-qv3);
    2.3. U=V, V=T.
  3. U=(ЕҮОБ(a,b),x,y)).
Соңы.
```

Алгоритм аяқталғаннан кейін нәтижесі *U* жолында болады. Алгоритмдағы div операциясы – бұл бүтін сандық бөлу операция.

Мысалы. *a* = 18, *b* = 9 болсын. Теңдеуге сай келетін *x* және *y* сандарды іздеп табайық

$$18x + 9y = \text{ЕҮОБ}(18,9).$$

Алгоритмды қадам бойынша орындайық:

q	U			V			T		
	u_1	u_2	u_3	v_1	v_2	v_3	t_1	t_2	t_3
18 div 9 = 2	18	1	0	9	0	1	18 mod 9 = 0	1 - 2·0 = 1	0 - 2·1 = -2
	9	0	1	0	1	-2			

Нәтижесінде аламыз U = (ЕҮОБ(a,b),x,y)) = (9,0,1).
Тексереміз: 18·0 + 9·1 = 9 = ЕҮОБ(18,9).

10.8 Модулі *m* бойынша инверсия

Криптографияның көптеген есептерінде берілген c, m сандар үшін іздеп табу керек $d < m$ санды, ол үшін

$$cd \bmod m = 1.$$

Осындай d болады тек сонда ғана, егер c мен m сандар өзара жай болатын болса.

cd mod m=1 теңдеуге сай келетін d саны, **модулі** m **бойынша** c-ң **инверсиясы** деп аталады және жиі белгіленеді c^{-1} mod m. Инверсия үшін берілген белгіле cd mod m=1 теңдеуді былай жазуға болатынымен байланысты

$$cc^{-1} \bmod m = 1.$$

Сонымен, модулі m бойынша есептеулерде c^{-1}-ге көбейту c-ға бөлуге сәйкес болады.

Модулі m бойынша инверсияны Евклидтың жалпыланған алгоритмы көмегімен де есептеуге болады.

Мұны көрсетейік. Төменірек жазылған теңдеудің мағынасы – кейбір бүтін k үшін $cd - km = 1$ теңдеу орын алады. c мен d өзара жай болатының еске алып, бұл теңдеуді келесі түрде өзгертуге болады:

$$m(-k) + cd = \text{ЕҮОБ}(m, c).$$

Демек, біз Евклидтың жалпыланған алгоритмы көмегімен c^{-1} mod m (немесе d санды табу) есептей аламыз. Бұл кезде айнымалы k мәні бізге керек емес. Егер d саны теріс болып табылса, онда оған m қосу керек, өйткені анықтама бойынша a mod m саны {0,1,...,m-1}жиыннан алынады.

Мысал қарастырайық. m=9, c=5 болсын. 5^{-1} mod 9 табайық. Барлық есептеуді қадам бойынша жазып отырып, Евклидтың жалпыланған алгоритмы бойынша есептеуді жүргізейік.

q	U			V			T		
	u_1	u_2	u_3	v_1	v_2	v_3	t_1	t_2	t_3
9 div 5 = 1	9	1	0	5	0	1	9 mod 5 = 4	1 - 1·0 = 1	0 - 1·1 = -1
5 div 4 = 1	5	0	1	4	1	-1	5 mod 4 = 1	0 - 1·1 = -1	1 - 1·(-1) = 2
4 div 1 = 4	4	1	-1	1	-1	2	4 mod 1 = 0	1 - 4·0 = 1	-1 - 4·2 = 7
	1	-1	2	0	1	7			

Сонымен, аламыз 5^{-1} mod 9 = 2. Тексереміз: 5·2 mod 9 = 10 mod 9 = 1.

Негізгі терминдер

Евклид алгоритмы – екі санның ең үлкен ортақ бөлгішін іздеп табуға мүмкін беретін математикалық алгоритм.

Өзара жай сандар – ортақ бөлгіштері жоқ (бірден басқа) сандар.

Факторизациялау есебі – көбейткенде берілген санды беретін екі не одан көп натурал сандарды табу.

Модулі бойынша инверсия – берілген санға модуль бойынша көбейткенде нәтижесінде бірді беретің натурал сан.

Көбейткіштерге канондық жіктеу - барлық көбейткіштер жай болып өсу ретінде жазылған көбейткіштерге жіктеу.

Ферманың кіші теоремасы – RSA жүйесі бойынша шифрлаудың негізінде жататын танымал теоремасы.

а мен *b* сандардың **ең үлкен ортақ бөлгіші** - *a*-ны да *b*-ны да бөлетін ең үлкен *c* саны: *c* = ЕҮОБ(*a*, *b*).

Арифметиканың негізгі теоремасы - кез келген бірден үлкен натурал сан не өзі жай болады, не жай бөлгіштердің көбейтіндісіне жалғыз ғана тәсілмен жіктелу мүмкін (егер көбейткіштердің жол ретін еске алмайтын болсақ).

Жай сан - өзінен және бірден басқа бөлгіштері болмайтын натурал сан. **Құрама сан** - өзінен және бірден басқа тағы да бір санға бөлінетің натурал сан. **Эйлер функциясы** - *n*-нан аспайтын және *n*-мен өзара жай болатын натурал сандардың санын есептеуге мүмкіндік беретін функция. Белгіленеді φ(*n*).

Сұрақтар

1. Жай және құрама санның анықтамасын беріңіз. Жай және құрама сандарының үш-үштен мысалдарын келтіріңіз.
2. «Өзара жай сандар» ұғымының анықтамасын беріңіз. Өзара жай сандардың және өзара жай болмайтын сандардың мысалдарын келтіріңіз.
3. Арифметиканың негізгі теоремасын тұжырымдап беріңіз.
4. Факторизациялау есебі деген не?
5. Ең үлкен ортақ бөлгіші анықтамасын беріңіз.
6. Екі санның ең үлкен ортақ бөлгішін табу үшін Евклид алгоритмды тұжырымдап беріңіз.
7. Ферманың кіші теоремасын тұжырымдап беріңіз.
8. Ферма-Эйлер теоремасын тұжырымдап беріңіз (RSA жүйесінің жағдайы үшін).
9. Жалпыланған (кеңейтілген) Евклид алгоритмын тұжырымдап беріңіз.
10. «Модуль бойынша алу операцияны» орындау принциптерін тұжырымдап беріңіз. Осы операцияның орындау мысалдарын келтіріп түсіндіріп беріңіз.
11. Модулі *n* бойынша инверсия деген не?