• көп таңбалы санды дәрежелеумен байланысты шифрлау және шифрды ашу процедуралары өте қиын.

Сондықтан әдетте ашық кілтті криптожүйелердің жылдамдығы құпия кілтті симметриялық криптожүйелердің жылдамдығынан жүздеген, мыңдаған есе көп.

Аралас (гибридті) шифрлау әдісі ашық кілтті асимметриялы криптожүйелердің жоғарғы қауіпсіздігіне және құпия кілтті симметриялы криптожүйелердің жұмыс жылдамдығының тездігіне негізделген. Ол кезде ашық кілтті криптожүйе шифрлау, біреуге беру және симметриялы криптожүйнің тек құпия кілтін ашу үшін қолданылады. Ал симметриялық криптожүйе алғашқы ашық мәтінді шифрлау және оны керекті жерге жіберу үшін қолданылады. Нәтижесінде ашық кілтті криптожүйе симметриялы криптожүйемен алмастырмайды, тек берілетін хабардың қауіпсіздігін жоғарылатуға болатындай жағдайда қолданылады.

Егер A пайдаланушы аралас әдіс арқылы шифрланған M хабарын B пайдаланушыға жібергісі келсе, оның әрекеті келесі тәртіппен орындалады:

1. Бұл әдісте сеанстық кілт деп аталатын, K_S симметриялық кілтті құру (мысалы, кез келген түрде генерациялау арқылы).

2. K_S сеанстық кілтінде M хабарын шифрлау.

3. B пайдаланушының K_B ашық кілтінде және өзінің k_A құпия кілтінде K_S сеанстық кілтін шифрлау.

4. Ашық байланыс арна арқылы B пайдаланушының мекен-жайына шифрланған хабар мен шифрланған сеанстық кілтін жіберу.

B пайдаланушы шифрланған хабарды және шифрланған сеанстық кілтті алған соң, оның әрекеті кері болуы тиіс:

5. Өзінің k_B құпия кілтінде және A пайдаланушының K_A ашық кілтінде K_S сеанстық кілтін ашу.

6. Алынған K_S сеанстық кілт арқылы M хабарын ашу және оқу.

Аралас шифрлау әдісін қолданғанда, тек B қолданушысы K_S кілтін дұрыс ашып, M хабарын оқи алатынына күмән жоқ.

Сонымен, аралас шифрлау әдісінде симметриялы криптожүйелердің және асимметриялы криптожүйелердің де криптографиялық кілттері қолданылады. Әрбір криптожүйенің түріне сәйкес кілттің ұзындығы аралас криптожүйнің кез келген қорғау

механизміне қарсыластың шабуылы қиын болатындай таңдалуы керек екендігі айқын.

14-кестеде толық таңдамалы шабуылының қиындығы сәйкес асимметриялық криптожүйелердің модульдерінің факторизациялауына тең болатын симметриялы және асимметриялы криптожүйелердің кілттерінің кең таралған ұзындықтары келтірілген.

14-кесте.

Криптомықтылығы бірдей симметриялы және асимметриялы криптожүйелердің кілттерінің ұзындықтары

Симметриялы криптожүйе кілтінің ұзындығы, бит	Асимметриялы криптожүйе кілтінің ұзындығы, бит
56	384
64	512
80	768
112	1792
128	2304

Аралас әдіс аутентификацияға, яғни берілетін кілттің дұрыстығын тексеру процедурасының орындалуына мүмкіндік береді. Ол үшін A қолданушы хабарды хэширлеу функцияның негізінде және өзінің k_A құпия кілті арқылы, белгілі электрондық цифрлық қолтаңба (ЭЦҚ) алгоритмінің көмегімен өз қолтаңбасын генерациялайды және оны қажеттіжерге жазады, мысалы жіберілетін файлдың соңына жазуға болады.

B пайдаланушы алынған хабарды оқып болған соң, абонентінің цифрлық қолының дұрыстығын тексере алады. B пайдаланушы қайта сол ЭЦҚ алгоритімін қолданып және келген хабарды хэширлеу нәтижесінде алынған қолтаңбаны тексереді. Аралас шифрлау әдісі тиімді болып табылады, мұнда симметриялық шифрлаудың жылдамдығы және ашық кілтті криптожүйелердің жоғары криптомықтылығы біріктірілген.

3.9. Асимметриялық криптожүйелердің салыстырмалы талдауы

RSA және Эль – Гамаль алгоритмдері пайдаланушылардың бір-бірімен өте тығыз байланыста болғандарын қажет етпейді. Месси-Омур алгоритмі диалогты қажет етеді де соның нәтижесінде оның қолдануына шектеу қояды.

Эль-Гамаль алгоритмінде шифр мәтіні алғашқы ашық мәтіннен екі есе ұзын. Сонымен қатар, бұл шифрлау алгоритмінде екі экспонент есептелінеді, ал RSA-да тек біреу, яғни RSA шифрлау алгоритмі екі есе жылдам орындалады. Эль-Гамаль және Месси-Омур алгоритмдерінің RSA-дан ерекшелігі, бірдей ашық мәтіндер әртүрлі шифр мәтіндеріне ауысады, ал бұл олардың статистикалық қасиеттерін зерттеуді қиындатады.

RSA алгоритмінің қауіпсіздігі құрамына санның жіктелуінің қиындығына, ал Эль-Гамаль хаттаманың қауіпсіздігі дискретті логарифмдеудің есептеуқиындығына негізделген.

RSA алгоритімінде, егер (e) шифрлау көрсеткіші аз сан болса, онда хабарды кілтсіз бұзып оқу қаупі орын алады. Екі жақтағы қолданушылар n модулінің жалпы мәнін бірдей қолданса, онда олардың құпия кілттерінің өзара ашылуына әкеледі.

Эль-Гамаль хаттамасында кілтсіз бұзып оқу болмау үшін кез келген k сандарын болжап таба алмайтындай және қайталанбайтындай болуы қажет.

Эль-Гамаль және Месси-Омур шифрлау алгоритмдері кез келген соңғы топ, мысалы, эллипс қисығының нүктелер тобы жағдайында жалпылануы мүмкін. Бірақ бұл жағдайда ашық мәтін топтың элементі болуы тиіс. Сондықтан шифрлау алгоритмі кез келген мәтінді топ элементіне түрлендіру кезеңін (шифрлауда) және кері (ашуда) кезеңді ескеру керек.

3.10. Экспонентті модуль бойынша есептеу

Экспонентті модуль бойынша есептеудің алғашқы ережесі:

$$C := M^e \pmod{n}.$$

Дәрежені есептеудің әр қадамында кез келген аралық нәтижені n модулі бойынша келтірілген дұрыс. Себебі, M^e екілік саны үшін

жадыға қойылатын талаптар өте жоғары. M және e әрқайсысы 256 бит болады деп есептесек, M^e-н сақтау үшін келесідей бит қажет:

$$\log_2\left(M^e\right) = e \cdot \log_2(M) \approx 2^{256} \cdot 256 = 2^{264} \approx 10^{80}.$$

Бұл сан шамамен әлемдегі бөлшектер санына тең, бізде оны сақтауға мүмкіндік жоқ. Осыған орай, жер бетіндегі барлық компьютерлердің биттік мүмкіндіктерін есептеу үшін біз жалпы ұсыныс жасайық: 512 млн. компьютер және әрқайсысында 512 Мб жады болсын. Онда биттердегі барлық жады келесіге тең болар еді:

$$512 \cdot 2^{20} \cdot 512 \cdot 2^{20} \cdot 8 = 2^{61} \approx 10^{18}$$

Бұл мән M^e-н сақтау үшін жеткілікті тек сол жағдайда, егер M және e 55 бит мәніне ие болса [1-28].

3.10.1. Экспонентті есептеу

Келесі сұрақ қойылады: $M^e \pmod n$-н есептеу үшін модуль бойынша қанша көбейту амалдарын орындау керек? $C = M^e \pmod n$ есептеу үшін ең қарапайым жол $C := M \pmod n$ бастап, тізбектей модуль бойынша көбейту амалдарын орындау:

$$C := C \cdot M \pmod n,$$

яғни, $C := M^e \pmod n$ мәнін алғанға дейін жүргіземіз. Бұл қарапайым әдіс $C := M^e \pmod n$ есептеу үшін модуль бойынша $e-1$ көбейтулерін қажет етеді, ол көптеген e үшін қиын. Мысалы, егер бізге $M^{15} \pmod n$-н есептеу қажет болса, бұл әдіс 15-ке дейін M-нің барлық дәрежелерін есептейді:

$$M \to M^2 \to M^3 \to M^4 \to M^5 \to M^6 \to M^7 \to \ldots \to M^{15}$$

Бұл 14 көбейту амалын қажет етеді. Бірақ M^{15}-н алу үшін барлық дәрежелерді есептеудің қажеттігі жоқ. Әрі қарай M^{15}-н есептеудің тез әдісі көрсетілген:

$$M \to M^2 \to M^3 \to M^5 \to M^7 \to M^{14} \to M^{15}$$

Мұнда тек 6 көбейту амалдарын орындау қажет. M^{15} есептелген әдіс белгілі бір көрсеткіштер үшін ғана емес, оны кез келген e үшін M^e-н есептеуге пайдалануға болады. Бұл әдіс бинарлық әдіс немесе квадратқа шығарып, көбейте бер әдісі деп аталады.

3.10.2. Бинарлық әдіс

Бинарлық әдіс көрсеткіш биттерін солдан оңға немесе оңнан солға көшіру болып табылады. Квадратқа шығару әр қадамда жасалады. Төменде біз солдан оңға қарай көшіру бинарлық әдісін қарастырамыз. Оңнан солға алгоритмі M дәрежелерін сақтауға қажетті айнымалыны қажет етеді. k-e үшін қажетті биттер саны болсын, яғни $k = 1 + \lfloor \log_2 e \rfloor$ және e-ң екілік бөлінуі берілген:

$$e = (e_{k-1} e_{k-2} \ldots e_1 e_0) = \sum_{i=0}^{k-1} e_i 2^i,$$

мұндағы $e_i \in \{0,1\}$. Сонда $C = M^e (\mathrm{mod}\, n)$ есептеу үшін бинарлық әдіс келесідей болады:

Бинарлық әдіс
Кіріс: M, e, n.
Шығыс: $C = M^e (\mathrm{mod}\, n)$.

1. егер $e_{k-1} = 1$ болса, онда $C := M$, әйтпесе $C := 1$
2. 0-ге дейін $i := k - 2$ үшін
2a. $C := C \cdot C (\mathrm{mod}\, n)$
2b. Егер $e_i = 1$, онда $C := C \cdot M (\mathrm{mod}\, n)$
3. C мәнін қайтару.

Мысалы, $e = 250 = (11111010)$, $k = 8$ болсын. Алғашқыда $C := M$ деп аламыз, себебі $e_{k-1} = e_7 = 1$.

Бинарлық әдіс келесі түрде орындалады:

i	e_i	2a қадамы	2b қадамы
6	1	$(M)^2 = M^2$	$M^2 \cdot M = M^3$
5	1	$(M^3)^2 = M^6$	$M^6 \cdot M = M^7$
4	1	$(M^7)^2 = M^{14}$	$M^{14} \cdot M = M^{15}$
3	1	$(M^{15})^2 = M^{30}$	$M^{30} \cdot M = M^{31}$
2	0	$(M^{31})^2 = M^{62}$	M^{62}
1	1	$(M^{62})^2 = M^{124}$	$M^{124} \cdot M = M^{125}$
0	0	$(M^{125})^2 = M^{250}$	M^{250}

Бинарлық әдіспен M^{250} есебі үшін модуль бойынша көбейту амалдарының саны 7+5=12. $e\ e_{k-1} = 1$ тең болғанда, бинарлық әдіс келесіні талап етеді:

- Квадратқа шығару (2a қадамы): $k-1$, мұндағы k - e -ның екілік бөлуіндегі биттер саны.
- Көбейту амалдарын талап етеді (2b қадамы): $H(e)-1$, мұндағы $H(e)$ - e санының Hamming-салмағы.

$e > 0$ деп есептей отырып, мынаған ие боламыз: $0 \le H(e)-1 \le k-1$. Осылайша,

$e_{k-1} = 1$, көбейту амалдарының жалпы саны былай бағаланады:

Ең үлкен: $(k-1)+(k-1) = 2(k-1),$

Ең кіші: $(k-1)+0 = (k-1),$

Орташа: $(k-1)+\frac{1}{2}(k-1) = \frac{3}{2}(k-1).$

3.10.3. m - арлы әдіс

Бинарлық әдісте e көрсеткіші тізбектеліп бір бит бойынша көшіріледі. 2 бит бойынша көшірсек, кватеринарлы, үшеуден болса, онда октальды әдісті аламыз және т.с.с.

Егер $\log_2 m$ бит бойынша көшірсек, мұндай әдіс m -арлы деп аталады.

m -арлы әдіс көрсеткіштің m -арлы бөлуіне негізделеді, оларға сәйкес e цифрлары көшіріліп, кейін квадратқа шығарылып, қажетті көбейтулер орындалады. m 2-нің дәрежесі болса, m -арлы әдісті жүзеге асыру қарапайым болып табылады, себебі M^e e көрсеткішінің екілік бөлуінде биттердің топтасуымен есептеледі. $e = (e_{k-1}e_{k-2}\ldots e_1e_0)$

көрсеткіші r бит бойынша s блоктан тұратын $sr = k$ тең болғандағы көрсеткіштің екілік бөлуі болып табылады. Былай анықтаймыз:

$$F_i = (e_{ir+r-1}e_{ir+r-2}\ldots e_{ir}) = \sum_{j=0}^{r-1} e_{ir+j}2^j.$$

$0 \le F_i \le m-1$ және $e = \sum_{i=0}^{j-1} F_i 2^{ir}$ екенін атап өтейік.

m-арлы әдіс $\omega = 2,3,...,m-1$ үшін бірінші $M^{\omega}(\mathrm{mod}n)$ есептейді. Кейін e екілік разрядтары одан соң r разрядтары бойынша бірден көшіріледі. Әр қадамда алдындағы нәтиже 2^r дәрежесіне шығарылып, n модулі бойынша M^{F_i}-ге көбейтіледі, мұндағы M^{F_i}-ағымдағы битсекцияның нөлдік емес мәні.

m-арлы әдіс

Кірісінде: M, e, n

Шығысында: $C = M^e \bmod n$

1. Барлық $\omega = 2,3,...,m-1$ үшін $M^{\omega}(\mathrm{mod}n)$ есептеп, сақтау керек
2. $i = 0,1,2,...,s-1$ үшін r-битті F_i сөзіне
3. $C = M^{F_i}(\mathrm{mod}n)$
4. $i = s-2$ үшін 0-ге дейін

4a. $C : C^{2^r}(\mathrm{mod}n)$

4b. егер $F_i \neq 0$ болса, онда $C := C \cdot M^{F_i}(\mathrm{mod}n)$

5. C мәнін қайтару.

3.10.4. Кватернарлық әдіс

Енді кватернарлық әдісті қарастырайық. e көрсеткішінің разрядтары бір өткенде екі рет көшірілгендіктен, мұндай мәндерді алуға болады: $(00) = 0, (01) = 1, (10) = 2, (11) = 3.$ Көбейту қадамында $M^0, M, ^1 M^2, M^3$ мәндері керек болуы мүмкін. Осылайша, M^2 және M^3 алу үшін кейбір алдын ала есептеулерді жүргізген дұрыс. Мысал үшін $e = 250$ тең болсын және e-ны екі разряд бойынша топтарға бөлу былай беріледі:

$$e = 250 = 11\,11\,10\,10.$$

Сонымен, $s = 4$ болды. Алдын ала есептеу қадамында төмендегіні есептейді.

Разрядтар	ω	M^{ω}
00	0	1
01	1	M
10	2	$M \cdot M = M^2$
11	3	$M^2 \cdot M = M^3$

Кватернарлық әдіс келесідей түрленеді: $C := M^{F_3} = M^3 (\mathrm{mod} n)$ және $M^{250} (\mathrm{mod} n)$ есептеу төмендегідей орындалады:

F_i	4a қадамы	4b қадамы
11	$(M^3)^4 = M^{12}$	$M^{12} \cdot M^3 = M^{15}$
10	$(M^{15})^4 = M^{60}$	$M^{60} \cdot M^2 = M^{62}$
10	$(M^{62})^4 = M^{248}$	$M^{248} \cdot M^2 = M^{250}$

Бұл әдістегі көбейту амалдарының саны $M^{250} (\mathrm{mod} n)$ мынаған тең болады: 2+6+3=11.

3.10.5. Октадды әдіс

Бұл әдісте көрсеткіштің екілік берілуі топтарға үш разряд бойынша бөлінеді. Мысалы, $e = 250$ көрсеткіші үшін мұндай бөлу сол жақтан бір нөл қосқанда келесі түрде болады:

$$e = 250 = \underline{001}\,\underline{111}\,\underline{010}$$

Бұл жағдайда: $s = k / r = 9 / 3 = 3$.

Алдын ала есептеу қадамында барлық $\omega = 2,3,4,5,6,7$ үшін $M^{\omega} (\mathrm{mod} n)$-ді есептейміз.

Разрядтар	ω	M^{ω}
000	0	1
001	1	M
010	2	$M \cdot M = M^2$
011	3	$M^2 \cdot M = M^3$
100	4	$M^3 \cdot M = M^4$
101	5	$M^4 \cdot M = M^5$
110	6	$M^5 \cdot M = M^6$
111	7	$M^6 \cdot M = M^7$

Октaлды әдіс келесі түрде түрленеді: $C := M^{F_2} = M^3 (\mathrm{mod} n)$, ал $M^{250} (\mathrm{mod} n)$ есептеу келесідей түрде жүргізіледі:

i	F_i	4a қадамы	4b қадамы
1	111	$(M^3)^8 = M^{24}$	$M^{24} \cdot M^7 = M^{31}$
0	010	$(M^{31}) = M^{248}$	$M^{248} \cdot M^2 = M^{250}$

Октaлды әдіспен $M^{250} (\mathrm{mod} n)$ есептеу үшін модуль бойынша 6+6+2=14 көбейту амалы қажет. Бірақ $\omega = 2,3,4,5,6,7$ үшін $M^{\omega} (\mathrm{mod} n)$ көрсеткіштерінің барлығы бірдей қолданылған жоқ. Сәйкесінше, $m-$ арлы әдістің 1-қадамын аз ғана түрлендіріп, $M^{\omega} (\mathrm{mod} n)$ алдын ала есептеулерін жүргізу керек. Мысалы, $e = 250$ үшін мынадай мәндер болады: $(011) = 3, (111) = 7, (010) = 2.$ Олар үшін дәрежелерді төрт көбейту амалдарының көмегімен таба аламыз:

Разрядтар	ω	M^{ω}
000	0	1
001	1	M
010	2	$M \cdot M = M^2$
011	3	$M^2 \cdot M = M^3$
100	4	$M^3 \cdot M = M^4$
111	7	$M^4 \cdot M^3 = M^7$

Октадды әдіске қажетті $M^{250}(\mathrm{mod}n)$ есептеу үшін жалпы санды береді, ол мынаған тең: 4+6+2=12. $M^{\omega}(\mathrm{mod}n)$ алдын ала есептеуі ω үшін ғана $M^{e}(\mathrm{mod}n)$ есептеу әдісі адаптивті немесе кірістегі мәліметтерге тәуелді алгоритм деп аталады. Келесі бөлімде берілген e көрсеткішінің қасиеттерін қолдана отырып, көбейту амалдарының санын азайтуға мүмкіндік беретін тәсілдерді қарастырамыз. Жалпы жағдайда көптеген k мәндеріне тән $\omega = 2,3,...,2^r - 1$ үшін $M^{\omega}(\mathrm{mod}n)$-ді есептеуіміз қажет болады. Енді m-арлы әдіске қажетті көбейту амалдарының орта санын бағалайық, $2^r = m$ және k/r-бүтін сан деп алайық [7].

- Алдын ала есептеу қадамындағы көбейту амалдарының саны (1-қадам): $m - 2 = 2^r - 2$
- Квадратқа шығарғандағы саны (4a-қадам): $\left(\frac{k}{r} - 1\right) \cdot r = k - r$
- Көбейту амалдарының саны (4b-қадам): $\left(\frac{k}{r} - 1\right) \cdot \left(1 - \frac{1}{m}\right) = \left(\frac{k}{r} - 1\right) \cdot \left(1 - 2^{-r}\right)$

Жалпы m-арлы әдісте орташа

$$2^r - 2 + k - r + \left(\frac{k}{r} - 1\right)\left(1 - 2^{-r}\right)$$

көбейту амалдары мен дәрежеге шығарулар қажет болады. Бинарлық әдісте көбейту амалдары мен дәрежеге шығарулардың орташа саны $r = 1\ m = 2$ есебінен алынған; бұл $\frac{3}{2}(k-1)$ береді. Әр k үшін тиімді мән $r = r^*$, m-арлы әдісте көбейту амалдарының орташа саны минималды болады. r-дің тиімді мәндері есептеу арқылы табылады. Кестеде бинарлық әдіс және r тиімді мәні бар m-арлы әдісі үшін көбейту амалдары мен квадратқа шығарудың орташа санының мәндері келтірілген.

k	Бинарлық	m-арлы	r	Үнемдеу, %
8	11	10	2	9,1
16	23	21	2	8,6
32	47	43	2,3	8,5
64	95	85	3	10,5