Електротехнички факултет у Београду

Семинарски рад из предмета САО

Дифи-Хелманов протокол размене

Грегор Стојковић 2018/0643

Професори:
Проф. др Бранко Малешевић, Проф. др Ивана Јововић
Проф. др Татјана Лутовац

18. септембар 2020.

Садржај

1 Увод **2**

2 Модуларна аритметика **3**
2.1 Конгруенција 3
2.2 Примитивни корен по модулу 4
2.2.1 Ојлерова функција 4
2.2.2 Ојлерова теорема 4
2.2.3 Ред броја по модулу 5
2.2.4 Примитивни корен 5

3 Дифи-Хелманов протокол **6**
3.1 Практичан пример процеса 6
3.2 Генерализација процеса 7
3.3 Дифи-Хелманов протокол са више учесника 9
3.4 Проблем аутентификације 10
3.5 Безбедност данас (RSA криптосистем) 11

4 Закључак **13**

5 Литература **14**

6 Прилози **15**

1 Увод

Дифи-Хелманов протокол размене (енг. DHKEP - Diffie-Hellman key exchange protocol) је метода успостављања
заједничког криптографског кључа у форми броја на "јавним" каналима.

Ова метода је једна од првих метода размена крипто кључева
преко јавних канала, објављена 1976. од стране Витфилд Дифиа и
Мартин Хелмана.

Идеја је да неке две особе, које не морају да се знају пре размене, могу без обзира на присуство неке трће особе која прислушкује, на безбедан начин да успоставе заједнички кључ за даљу комуникацију. При овој размени, све информације које размењују те две особе чује и она која прислушкује. Међутим, са снабдевеним информацијама, прислушкивач не може да манипулише тако да и он добије исти кључ.

Данас се Дифи-Хелманов протокол користи устаљено за све форме комуникације два уређаја преко интернета или неких других сервера, који, уз још неке методе енкрипције, омогућава безбедан проток
информација од пошиљиоца до примаоца.

Цео процес се заснива на области дискретне математике која се зове модуларна аритметика.

2 Модуларна аритметика

Као што смо већ поменули, цео процес Дифи-Хелмановог протокола се базира на области математике која се зове модуларна аритметика па да наведемо и дефинишемо неколико појмова који ће нам требати при разумевању математике иза овог процеса.

2.1 Конгруенција

У модуларној аритметици се врше операције сабирања по модулу и множења по модулу над коначним пољем целих бројева. Међутим, у овом раду ћемо посматрати само проширени скуп природних бројева $\mathbb{N}_0$.
Операције сабирање по модулу и множење по модулу су стандардне операције сабирања и множења, само што, када се дође до неке одређене вредности n, након ње почињемо опет од нуле.

Сходно томе, за бројеве a и b ($(a, b) \in \mathbb{N}_0$) кажемо да су конгруентни у ознаци

$a \equiv b \ (mod \ n)$

ако њихова разлика дели n (односно $a - b = kn, \quad k \in \mathbb{Z}$).
Такође, исто се може написати као:

$$a = kn + b$$

Друга интерпретација конгруенције је, ако важи $a \equiv b \ (mod \ n)$, то значи да a и b имају исти остатак при дељењу са n, односно:

$$a = kn + r$$
$$b = kn + r$$

На основу овог примера можемо дефинисати операцију модулирања као:

$$a \ mod \ n = r$$

2.2 Примитивни корен по модулу

Пре него што дефинишемо примитивни корен по модулу, треба прво дефинисати неколико ставки.

2.2.1 Ојлерова функција

Дефинишимо *редуковани систем остатака по модулу* n.
Редуковани систем остатака по модулу n је скуп природних бројева R за који важи да је НЗД$(r_i, n) = 1, \quad r_i \in R \mid r_i \not\equiv r_j,\ (i,j) \in \mathbb{N} \wedge (i \neq j)$ и $(\forall x \in \mathbb{N})(\exists r \in R) \quad x \equiv r\ (mod\ n)$.

Ојлерова функција је функција $\varphi : \mathbb{N} \to \mathbb{N}$ дефинисана са $\varphi(n) = card(R)$ где је R редуковани систем остатака по модулу n.
Другим речима, $\varphi(n) =$ број природних бројева узајамно простих са n, а мањих од n.

Лако се види да редуковани систем остатака по модулу p, где је p прост број, има $p-1$ чланова па је самим тим и $\varphi(p) = p - 1$.

2.2.2 Ојлерова теорема

Ојлерова теорема: Нека су $n \in \mathbb{N}$ и $a \in \mathbb{Z}$ узајамно прости бројеви, односно НЗД$(a, n) = 1$. Тада важи:

$$a^{\varphi(n)} \equiv 1\ (mod\ n)$$

Као последицу Ојлерове теореме, добијамо **Малу Фермаову Теорему** која каже да, ако је горе поменути број n прост број, тада важи да је:

$$a^{n-1} \equiv 1\ (mod\ n)$$

На основу Ојлерове теореме и Мале Фермаове теореме издвојимо закључак да за неки број $a \in \mathbb{N}$ и за неки прост број p важи:

$$\begin{aligned} a^{p} &\equiv a\ (mod\ p) \\ a^{p-1} &\equiv 1\ (mod\ p) \end{aligned} \tag{1}$$

2.2.3 Ред броја по модулу

Нека су a и n два узајамно проста природна броја. Најмањи број $d \in \mathbb{N}$ за који важи $a^d \equiv 1 \ (mod\ n)$ назива се ред броја a.
Ред броја a дели $\varphi(n)$, односно $d|\varphi(n)$.

2.2.4 Примитивни корен

Нека је g неки природни број мањи од n. Ако за број g важи да је његов ред по модулу n једнак $\varphi(n)$, тада се за њега каже да је он **примитивни корен по модулу** n.

На основу овога, можемо закључити да:

$$(\forall r \in R)(\exists k \in \mathbb{Z}) \quad g^k \equiv r \ (mod\ n)$$

где је g примитивни корен по модулу n и R редуковани систем остатака по модулу n.
Примитивни корен мора бити узајамно прост са n.
Примитивни корен по модулу n не мора бити јединствен.
Ако постоји бар један примитивни корен по модулу n, онда их постоји тачно $\varphi(\varphi(n))$.

3 Дифи-Хелманов протокол

3.1 Практичан пример процеса

Нека се у учионици налазе два студента (студент А и студент Б) и професор. Студенти се не знају међусобно од раније и довољно су удаљени један од другог да не могу размењивати папире и цедуљице, а довољно близу да могу да се чују док причају, али их и професор чује. Задатак је да студент А на папиру напише неку енкриптовану поруку такву да је студент Б може декриптовати, али не и професор, без обзира на то да је све информације које су студенти разменили до тад чуо и професор. Ово се лако може урадити коришћењем Дифи-Хелмановог протокола размене.

Једноставности ради, рећи ћемо да ће студенти разменити све информације и добити исти број k који ће студент А користити да енкриптује поруку тако што ће сва слова померити за k места удесно у азбучном поретку, с тим да, ако дође до слова Ш, само ће да настави бројање од А. Декрипција је само инверзно од тога, односно сва слова се померају за k места улево.
Размена информација се врши разговором између студената у присуству професора.
Порука коју ће студент А послати је "ТРАНСМИТАНСА".

Студент А ће студенту Б рећи два броја, број p који ћемо звати модул и број g који ћемо звати база. Нека је $p = 17$ и $g = 7$. Сада ова два броја знају сви у учионици. Студент А ће замислити неки број $a \in \{0, ..., 16\}$ који ће само он знати. Исто ће урадити и студент Б и добити свој број b. Нека је $a = 3$ и $b = 5$. Студент А ће узети базу и наћи $a_p = g^a \ mod \ p$, а студент Б $b_p = g^b \ mod \ p$. У овом случају добиће се да је $a_p = 3$, а $b_p = 11$. Студент А наглас изговори добијени број a_p, а студент Б b_p. Сада оба студента знају и a_p и b_p, али и професор. Последњи корак је да студент А нађе број $k_a = b_p^a \ mod \ 17$, а студент Б $k_b = a_p^b \ mod \ 17$. Увек ће се испоставити да је $k_a = k_b = k$. Добијени број k зове се кључ и у овом случају $k = 5$.
Све што сада студент А треба да уради је да помери сва слова оригиналне поруке 5 места удесно.

Оригинална порука је "ТРАНСМИТАНСА". На папиру, након помераја, студент А ће написати "ЦФЂСХРМЦЂСХЂ", при чему А=0, Б=1,..., Ш=29.
Овај папир затим професор узима и може да види садржај поруке, али

тешко да може и да је протумачи. Професор предаје папир студенту Б који само треба да помери сва слова за 5 места улево и, заиста, добија оригиналну поруку "ТРАНСМИТАНСА".

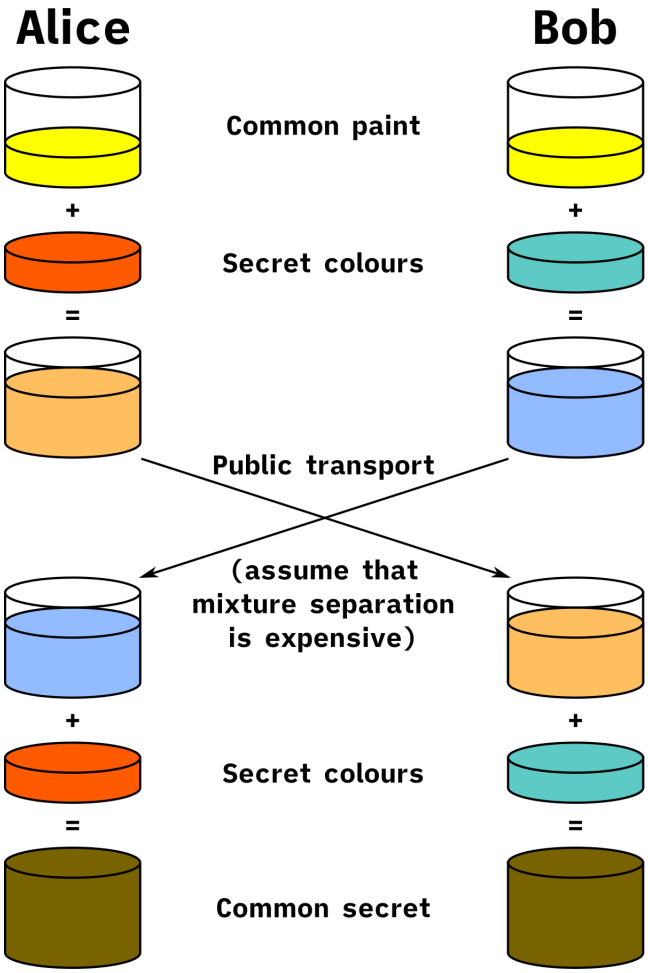
3.2 Генерализација процеса

Видели смо на конкретном примеру како функционише овај процес, а сада да појаснимо на општем нивоу логику иза тог процеса.

Прво се изабере циклична група G димензије p и неки елемент $g \in G$ који генерише G. У примеру смо бројеве p и g назвали модул и база респективно.
У пракси се узима много велики прост број p, углавном око 2000 бита, а данас и до 4000. Прост број се узима због његове особине да је $\varphi(p) = p-1$ па самим тим има $p-1$ потенцијалних примитивних корена по модулу p. Такође, на основу (1), особина простих бројева је да сигурно имају бар један примитивни корен па самим тим сигурно имају тачно $\varphi(\varphi(p))$ примитивних корена што је, за много велико p, широк избор.
Узимамо један примитивни корен по модулу p и бирамо га тако да и он буде прост и не мора бити велик. Изабран такав број је број g који заиста генерише G ($dim\ G = p$) по дефиницији.
Ова два броја су јавно позната и одавде креће процедура.

Прво се генришу два броја која нису јавно позната. Из наведеног примера то су бројеви a и b ($(a, b) \in \{0, ..., p-1\}$), при чему је број a познат само особи А, а b само особи Б.
Након тога, особа А јавно објави број g^a, а особа Б јавно објави g^b. Особа А затим (сад познат) број g^b дигне на a-ти степен односно добије $(g^b)^a$, а особа Б нађе $(g^a)^b$. Модулирањем са p, добија се $k = g^{ab}\ mod\ p$.

Уколико не постоји познат алгоритам да се нађе g^{ab} ако су познате све јавне информације (p, g^a и g^b), а притом нису познате a и b, због величине броја p, иако могуће, претешко је наћи k.



Слика 1: Сликовито приказан Дифи-Хелманов протокол

Поред овако објашњене интерпретације Дифи-Хелмановог протокола, често се користи и визуелни пример мешања различитих боја тако да се на крају дође до исте (слика 1).

Овде се лако види да било ко ко дође у контакт са разменом добија бројеве p, g, g^a и g^b, од којих никако не може наћи $k = g^{ab}\ mod\ p$ без знања бар једног од бројева a и b.

Међутим, ова процедура се не мора односити искључиво на случај када ДВЕ особе покушавају доћи до истог кључа.

3.3 Дифи-Хелманов протокол са више учесника

Логика се може проширити и на више од два учесника.
Узмимо на пример три учесника, особу А, особу Б и сад особу Ц, која ће такође учествовати у размени.

Исто као и раније, свака особа замисли само свој јединствен број. Нека су то бројеви a, b и c за особе А, Б и Ц респективно. Исто као и раније, постоје већ познати бројеви p и g. Особа А нађе g^a и проследи је особи Б која нађе $(g^a)^b$ и проследи је особи Ц која коначно нађе g^{abc}.
Потом особа Ц проследи особи А g^c, која проследи особи Б $(g^c)^a$ како би и она добила g^{abc}. Цео процес се опет понови за особу А.
У случају да је неко прислушкивао, једини бројеви које би тај неко могао иамти су p, g, g^a, g^b, g^c, g^{ab}, g^{ac} и g^{bc} са којима никако не може да дође до g^{abc}.
Како сада особе А, Б и Ц имају g^{abc}, сада могу наћи $k = g^{abc}\ mod\ p$.

Видимо да се овде може закључити да се овај процес може у најопштијем случају проширити на било који број учесника. Логика остаје иста.
Сваки учесник узима прво број g, диже га на свој степен и прослеђује наредном учеснику који добијени број опет диже на свој степен и прослеђује даље и тако $n-1$ пута (где је n број учесика). Затим, n-ти пут, сваки учесник добијени број последњи пут диже на свој степен и тако добија $g^{a_1 \cdot a_2 \cdot \ldots \cdot a_n}$. Налажењем модула p тог броја, добија се тражени број k.

Овако организовано, овај процес може потрајати дуго. Постоје различите методе оптимизације да се смањи време процеса и број корака (нпр: "divide-and-conquer-style"који смањује број операција на $log_2(n)+1$), али оне су опционе.
На крају се свакако долази до истог циља.

3.4 Проблем аутентификације

Објаснили смо да је Дифи-Хелманов протокол одличан процес за долажење до истог кључа између неке две стране, али није нужно да се комуникација преко заједничког кључа успоставила баш између страна због којих се покренуо овај протокол.
Другим речима, Дифи-Хелман не пружа гаранцију аутентичности.

Посматрајмо ситуацију где страна А жели успоставити комуникацију са страном Б преко неког сервера. Једноставности ради, нека тај сервер само прослеђује поруку од А до Б, без неких додатних фактора безбедности. У случају да је тај сервер хакован од стране особе Ц, особа Ц може при успостављању кључа да се понаша као страна Б.

Страна А шаље преко сервера страни Б свој g^a. Међутим, особа Ц заустави пренос поруке и нареди серверу да уместо да проследи поруку страни Б, генерише број c и врати $k_a = g^{ac}$ страни А, а страни Б пошаље g^c и заузврат добија $k_b = g^{bc}$. Сада стране А и Б мисле да су успоставиле заједнички кључ и безбедну комуникацију, али заправо, комуницирају преко трће стране за коју ни не знају.

Када особа А коришћењем Дифи-Хелмана енкриптује своју поруку и пошаље је серверу, особа Ц мора да је декриптује својим k_a кључем, затим да је опет енкриптује, али сада коришћењем k_b кључа и проследи је особи Б.
Током тог процеса у серверу, очигледно је да особа Ц има приступ поруци која се шаље и да може њом да манипулише, ако то жели, или само да је чита, што потпуно уништава сврху Дифи-Хелмановог протокола.

Због оваквог проблема, а и због ефикасности овог процеса, Дифи-Хелманов протокол се користи у комбинацији са додатним методама енкрипције (нпр. RSA криптосистем) као форма аутентификације страна које комуницирају.

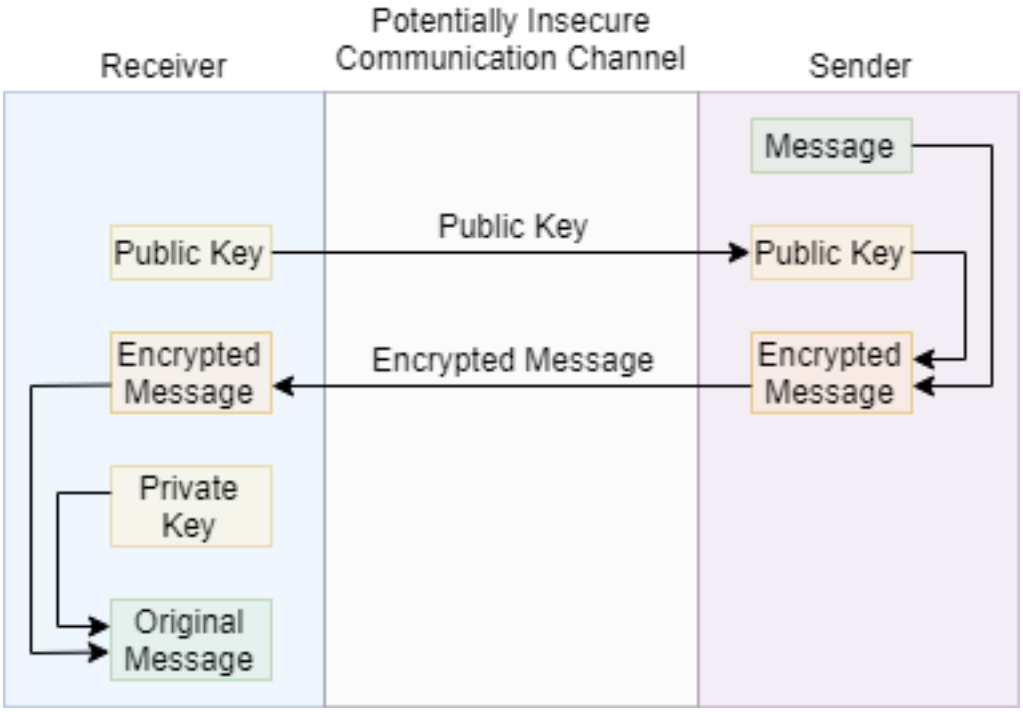
3.5 Безбедност данас (RSA криптосистем)

У претходној секцији смо показали пример да не мора да се нађе заједнички кључ између две стране, него само треба глумити једну од те две при успостави комуникације да се безбедност заобиђе. Међутим, може се при декриптовању потврдити аутентичност поруке и потврдити гаранција да ју је послала особа од које се порука очеквала.
Као у сфери пре компјутера, аутентичност поруке се потврђивала воском и печатом притиснутим на восак који је служио као лепак да се порука не може прочитати без оштећења воска. У зависности од печата можемо закључити да је писмо послато од стрне особе која једина има тај печат, а са сигурношћу можемо тврдити да порука није мењана у међувремену на основу тога да ли је восак поломљен или не.
Данас то радимо преко "дигиталног потписа".

Један од форми дигиталних потписа може бити RSA(Rivest-Shamir-Adleman) криптосистем који се може посматрати као систем кључева.

Наиме, свака страна која учествује у некој размени информација, пре било каквих интеракција, генерише два кључа. Један кључ ћемо звати "јавни кључ"(у ознаци k_j), а други ћемо звати "приватни кључ"(у ознаци k_p). Приступ јавном кључу, као што име налаже, има свако ко учествује у комуникацији и зна се којој страни припада сваки кључ. Други приватни кључ има само једна страна која учествује у комуникацији и њој нема приступ нико други. Ова два кључа чине пар за који важи да све што је "закључано"једним од њих, може се "откључати"другим, али не и да се истим кључем и закључа и откључа. На овај начин се обезбеђује аутентичност поруке објашњен на следећем примеру:

Страна А генерише свој пар кључева k_{pa} и k_{ja}, где k_{pa} зна само страна А, док је k_{ja} јавно објављена. Исто уради и страна Б. Страна А шаље поруку страни Б. То чини тако што ће своју поруку да "закључа"(енкриптује) коришћењем јавно познатог кључа k_{jb}, и то потом преко јавних сервера да пошаље страни Б. Поруку коју добије, страна Б откључава својим приватним кључем k_{pb} (слика 2). Уколико у томе успе, страна Б гарантује да порука у процесу доставе није мењана због особине да се порука може откључати једним кључем ако и само ако је закључана другим.



Слика 2: Шема RSA криптосистема

Овај процес размене гарантује аутентичност поруке, али не гарантује да је дошла од стране с којом мислимо да комуницирамо. То се може исправити на седећи начин.

Исто као и у претходном примеру, страна А генерише свој пар кључева (k_{pa} и k_{ja}) и страна Б своје (k_{pb} и k_{jb}). Уколико страна А своју поруку прво закључа својим приватним кључем k_{pa}, а потом јавним кључем k_{jb} стране Б па тек онда пошаље поруку, страна Б је може прочитати ако и само ако има свој приватни кључ k_{pb}, а потврђује да је поруку постала страна А тако што ће користити и јавни кључ k_{ja} стране А да дође до оригиналне поруке. Ако у туме успе, страна Б гарантује да је порука аутентична и сигурно послата од стране стране А јер ју је откључала коришћењем кључа k_{ja} што је једино могуће уколико је порука првом била закључана коришћењем кључа k_{pa}.

Дифи-Хелманов протокол у комбинацији са RSA системом омогућава безбедну успоставу комуникације двеју страна, а самим тим и безбедну даљу комуникацију.

4 Закључак

Дифи-Хелманов протокол размене је један од најранијих протокола безбедне јавне размене тајне. Развијањем информационих технологија и наглим напредовањем криптографије, Дифи-Хелманов протокол је и даље остао у основама размене информиација и до данас, што говори о ефикасности и једноставности овог протокола, али и о његовој безбедности. Како се криптографија развијала, тако су се развијале и методе које побољшавају безбедност у комбинацији са Дифи-Хелмановим протоколом (нпр. ECDHE_RSA_SC - elliptic curve Diffie-Hellman exchange RSA secure connection који користи Google Chrome) из чега можемо да закључимо да ћемо се још неко време ослањати на DHKEP.

Дифи-Хелманов протокол размене је само један од многих примера примене теорије бројева, самим тим и дискретне математике, који се користе свакодневно и без нашег нужног знања, а без којих би живот каквим га данас знамо био много другачији и, вероватно, компликованији.

5 Литература

1. Diffe W, Hellman ME. New Directions in Cryptography. IEEE Transactions on Information Theory 1976; 22(6):644-654
https://ee.stanford.edu/~hellman/publications/24.pdf

2. Hellman ME. An overview of public key cryptography. IEEE Communication Magazine 2002; 40(5):42-49
https://ee.stanford.edu/~hellman/publications/31.pdf

3. Душан Ђукић. Конгруенције вишег степена: https://imomath.com/srb/dodatne/stepene\%20kongruencije_ddj.pdf

4. Williamson MJ. Thoughts on cheaper non-secret encryption: https://www.fi.muni.cz/usr/matyas/lecture/paper3.pdf

5. Vinogradov IM. Primitive roots and indices: https://books.google.co.jp/books?id=xlIfdGPM9t4C&lpg=PR3&hl=ja&pg=PA105#v=onepage&q&f=false

6. Weisstein EW. Primitive root: https://mathworld.wolfram.com/PrimitiveRoot.html

7. Totient function. Encyclopedia of Mathematics: https://encyclopediaofmath.org/index.php?title=Totient_function

8. Secret Key Exchange (Diffie-Hellman) - Computerphile (https://www.youtube.com/watch?v=NmM9HA2MQGI&t=10s&ab_channel=Computerphile)

9. Key Exchange Problems - Computerphile (https://www.youtube.com/watch?v=vsXMMT2CqqE&ab_channel=Computerphile)

10. Хелманов говор о криптографији: DISI 2007: A Fool's Errand Inventing Public Key Cryptography (https://www.youtube.com/watch?v=zTGqP0nxX08&ab_channel=UPM)

11. Смајиловић М. Ојлерова теорема. Теорија бројева; Скрипта са предавања 2004/05: 47-51.

12. Смајиловић М. Примитивни коријен. Теорија бројева; Скрипта са предавања 2004/05: 51-55.

6 Прилози

Слика 1: https://en.wikipedia.org/wiki/Diffie\%E2\%80\%93Hellman_key_exchange#/media/File:Diffie-Hellman_Key_Exchange.svg

Слика 2: https://www.google.com/url?sa=i&url=https\%3A\%2F\%2Fmedium.com\%2F\%40jinkyulim96\%2Falgorithms-explained-rsa-encryption-9a37083aaa62&psig=AOvVaw3Di-GltFxzU5_er70fFtDq&ust=1600095014871000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCPiq-Mqw5usCFQAAAAAdAAAAABAD