DIFFIE HELLMAN

მახასიათებლები:

Diffie Hellaman - ის მეთოდი კრიპტოგრაფიაში ცნობილია არასიმეტრიული დაშიფვრის მექანიზმით. კერძოდ ის პასუხისმგებელია ისეთი გასაღების გენერირებაზე რომლის ნაწილებად დაშლა მესამე პირისათვის რთლი საქმე იქნება. სწორედ ამიტომ ქვია მას არასიმეტრიული მექანიზმი რადგან ხდება გასაღების გამოთვლა და ასევე არცერთმა მხარემ არ იცის მეორე მხარის იმერ ჩაფიქრებული პირადი გასაღები.

სანამ დასაშიფრი ინფორმაციის მიმოცვლა დაიწყება, ჯერ რამდენიმე ეტაპიანი გასაღების გამოთვლა ხდება.

|  |  |  |
| --- | --- | --- |
| პირი 1 | საერთო სივრცე/პირი 3 | პირი 2 |
| a | g p | b |
| ga mod p |  | gb mod p |
|  | ga mod p “ gb mod p |  |
| gb mod p |  | ga mod p |
| gbamod p | = | gab mod p |

იქიდან გამომდინარე, რომ გაგზავნილი ინფორმაციის ხელში ჩაგდება ჩეუძლია მესამე პირს, ვითვალისწინებთ რომ მან იცის ყველა ცვლადი რაც საერთო სივრცეშია.

თავდაპირველად ხდება გენერირება ორი g, და p რიცხვების. ზემოთხსენებული ალგორითმი გვთავაზობს, რომ საიმედოობისათვის p უნდა იყოს რაც შეიძლება დიდი მარტივი რიცხვი.

ამას შემდგომშ ავხსი რატომ.

მას შემდეგ, ორივე მხარე ახდენს გენერირებას ნებისმიერი შემთხვევითი რიცხვის. ამ რიხვს არანაირი შეზღუდვა არ აქვს. ამ მარტივი რიცხვის გენერირების შემდეგ, ორივე მხარე ახდენს თავიანთ შუალედური გასაღების გამოთვლას. ცნობილ g რიცხვი აჰყავთ ჩაფიქრებულ a რიცხვის ხარისხში და ითვლიან ნაშთს p ზე გაყოფისას. გასათვალისწინებელი და უმნიშვნელოვანესია რომ ნაშთები მიიღება [0 ; p) შუალედში. ამის შემდეგ ორივე მხარე ახდენს მიმოცვლას გამოთვლილი შუალედური გასაღებების. მეორე მხარის შუალედური გასაღების მიღების შემდეგ აჰყავს თავის მიერ ჩაფიქრებული რიცხვის ხარისხში და ორივე მხარე იღებს ერთსა და იმავე რიცხვს. იმი და მიუხედავად რომ არცერთმა არ იცის რა რიცხვი ჩაიფიქრა მეორემ.

მესამე პირისათვის კი გაგზავნის დროს ცნობილია მხოლოდ g, p, ga mod p , gb mod p.

მესამე პირმა რომ გაშფროს გაგზავნილი ინფორმაცია მან უნდა გაიგოს ან a ან b. რომლებიც დამალულები არიან გაგზავნილ ინფორმაციაში.

ეხლა ვისაუბროთ რატომ არის მათი ამოხსნა ესეთი რთული. მესამე პირმა მიიღო ერთ უცნობიანი განტოლება. ამოსახსნელად მან უნდა ამოხსნას დისკრეტული ლოგარითმული ამოცანა. და იმის გათვალისწინებით რომ p არის ძალიან დიდი მარტივი რიცხვი. ამ ამოცანის ამოხსნის ერთადერთი საშუალება არის რომ რიგრიგობით ცადოს. 1 დან p მდე რიცხვები იქნებ ცნობილი g ს ახარისხებით მიიღოს შედეგი. იმის გათვალისწინებით რომ დღევანდელ სუპერკომპიუტერსაც კი ძალიან დიდი დრო დასჭირდება ამ ამოცანის ამოსახსნელად. არავინ დარდობს ამ გასაღების სანდოობაზე.

|  |  |  |
| --- | --- | --- |
| პირი 1 | საერთო სივრცე/პირი 3 | პირი 2 |
| a = 4 | g = 5 p = 23 | b = 3 |
| 54 mod 23 = 4 |  | 53 mod 23 = 10 |
|  | 4 “ 10 |  |
| 10 |  | 4 |
| 104mod 23 = 18 | = | 43 mod 23 = 18 |

ზემოთ მოყვანილი მაგალითისას ავიღე რარაც რიცხვები და გამოვთვალე გასაღები.

რეალურ ცხოვრებაში 23 ძალიან პატარა მარტივი რიცხვია 50 ნიშნა მარტივი რიცხვები და უფრო დიდებიც გამოიყენება. 23 ის შემთხვევაში მარტივია გატეხვა. რადგან კომპიუტერს მოუწევს სცადოს რიცხვები რომლებიც 23 ზე პატარაა რაც საკმაოდ ცოტაა.

მას შემდეგ რაც გასაღები გამოთვლილია. უკვე ორივე მხარეს შეუძლია დაიწყოს ინფორმაციის დაშიფვრა დეშიფრაცია. და ასევე უკვე ვიცით რომ მესამე პირმა რომც ჩაიგდოს ხელში მას წარმოუდგენლად დიდი დრო დასჭირდება გასაშიფრად, რასაც რეალური კომპიუტერების შესაძლებლობისას გამოვრიცხავთ. ხოლო რეალური საბრთხე კვანტური კომპიუტერი იქნება, რომელსაც თეორიულად სწორედ ამ დისკრეტული ლოგარითმული პრობლემის ამოხსნას შეძლებს მცირე დროში.

მიღებულ გასაღებს ჯერ უნდა ვუპოვნოთ შებრუნებული გასაღები.

ამისათვის უნდა ამოვხსნათ განტოლება.

Key \* Key-1  = 1 mod (p - 1)

18 \* k-1 = 1 mod 22

შებრუნებული გვჭირდება იმაში რომ როდესაც ერთი დაშიფვრავს ინფომაციიას მეორემ შებრუნებულზე ახარისხებით იგივე მიიღოს. უხეშად რომ ვთქვათ მთავარმა და შებრუნებულმა გასაღებებმა ერთმანეთ უდნა გააბათილონ და პირველადი ინფორმაცია უნდა მოგვცეს.

იმის გამო რომ ცუდი გასაღები მივიღეთ და საერთო ჯერადი აქვთ 22 და 18. ვერ მოიძებნება მისი შებრუნებული მეწყვილე მთელ რიცხვთა სიმრავლეში.

მაგალითისათვის ავიღებ რაიმე სხვა რიცხვს. მაგალითისათვის იყოს გასაღები 5.

5 \* k-1 = 1 mod 22

k-1 = 9

ამ შემთხვევაში როდესაც წყვილის პოვნა ვერ ხერხდება ორივე მხარე თავიდან იფიქრებს რაიმე შემთხვევით რიცხვს. დავუშვათ ჩაიფიქრეს და გასაღები მიიღეს 5.

პირველ რიგში მოხდება დასაშიფრი ინფორმაციის ბაზასთან შესაბამისობა. ბაზას ავიღებ 1-26 ინგლისურ ასოებს.

“HI” დასაშიფრი სიტყვა „8 , 9“

85 mod 23 = 16 დაშიფვრა. 95 mod 23 = 8 დაშუფრული სიტყვა (16, 8) = ph

169 mod 23 = 8 წყვილის გამოყენებით დეშიფრაცია. 89 mod 23 = 9

როგორც ავღნიშნე ალგორითმი არის ძალიან საიმედო. ასევე ზემოთ ავღნიშნე შესაძლო შუალედები. რომ მიღებულლი შედეგები ჩაფიქრებული მარტივი რიცხვით არის შემოსაზღვრული და მარტივი რიცხვის ზომა განსაზღვრავს საიმედოობას.

საბოლოოდ მიღებული შედეგის კოდირება ხდება და მეტი სიმარტივისა და საიმედოობისათვის ორობით სისტემაში გადაგზავნა.რაც კიდევ უფრო ართულებს შიფრის გატეხვას. მაგრამ როგორც ავღნიშნე ამის გარეშეც უძლიერესი შიფრია. რომელიც რეალურად დღეს ფართოდ გამოიყენება, ყველგან ეს იქნება ბანკები თუ სოციალური ქსელები.

ადრე მქონდა პატარა ვიზუალიზაცია პრეზენტაციის სახით გაკეთებული ამ მეთოდით გასაღების მიღებასთან დაკავშირებით და იმასაც აგიტვირთავთ.