ზურაბ ქოჩლაძე

# ჰილის მოდიფიცირებული ალგორითმის გამოყენება თანამედროვე ბლოკურ შიფრებში უსაფრთხოების გაზრდის მიზნით.

(მოხსენება კომპიუტერული მეცნიერებების დეპარტამენტის რეგულარულ სამეცნიერო სემინარზე)

## მოკლე ანოტაცია


როგორც ცნობილია, ინფორმაციის კონფიდენციალურობის დასაცავად გამოიყენება სიმეტრიული ბლოკური ალგორითმები. მათემატიკურად ბლოკური შიფრი შეიძლება წარმოვიდგინოთ როგორც ორ ცვლადზე დამოკიდებული ფუნქცია

$$E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n \qquad (1)$$

სადაც $\{0,1\}^l$ აღნიშნავს $l$ სიგრძის ბიტურ სტრიქონს. $k$-ს და $n$-ს მნიშვნელობები კი დამოკიდებულია დაშიფვრის კონკრეტულ ალგორთმზე. პრაქტიკულად, თითოეული ფიქსირებული $K \in \{0,1\}^k$-თვის დაშიფვრის ფუნქცია წარმოადგენს გადანაცვლებას $\{0,1\}^n$-ზე.

თუ კრიპტოანალიტიკოსს მიზანია გამოთვალოს გასაღები, მაშინ ბლოკური შიფრების უსაფრთხოების ანალიზი შეიძლება ჩამოვაყალიბოთ შემდეგი ამოცანის სახით: მოცემულია დაშიფვრის ფუნქცია $E_k(M) = C$, სადაც $K \in \{0,1\}^k$ არის უცნობი გასაღები. ამ დროს კრიპტოანალიტიკოსისათვის ცნობილია შესასვლელი და გამოსასვლელი მნიშვნელობების რაიმე $q$ რაოდენობის წყვილები $(M_1, C_1),...(M_q, C_q)$ და ის ცდილობს გამოთვალოს გასაღები. ამ შემთხვევაში ბლოკური შიფრი იქნება უსაფრთხო, თუ საუკეთესო შეტევა, რომელიც შეუძლია განახორციელოს მოწინააღმდეგემ მოითხოვს ისეთი დიდი რაოდენობს $q$ წყვილებს ან/და გამოთვლის ისეთ დიდ $t$ დროს, რაც აღემატება კრიპტოანალიტიკოსის შესაძლებელობებს. ეს არის უსაფრთხოება გასაღების გამოთვლის მიმართ და იზომება რაოდენობრივად $q$ და $t$ პარამეტრების საშუალებით.

ის ფაქტი, რომ ბლოკური შიფრი უსაფრთხო იქნება გასაღების გამოთვლაზე შეტევებისადმი, სულაც არ ნიშნავს, რომ ის უსაფრთხო იქნება ზოგადად, რადგანაც, როგორც ჯერ კიდევ კ. შენონმა აჩვენა, ალგორითმი შეიძლება უშვებდეს რაიმე სახის ინფორმაციის გაჟონვას ღია ტექსტის შესახებ. ასეთ შემთხვევაში კრიპტოანალიტიკოსს უჩნდება შანსი საკმარისი რაოდენობის ინფორმაციის დაგროვების შემდეგ მთლიანად გატეხოს ალგორითმი. ამას ხელს უწყობს ისიც, რომ თავისი ბუნებით ბლოკური შიფრები წარმოადგენენ დეტერმინირებულ სისტემას, ანუ ერთი და იგივე ღია ტექსტი ერთი და იგივე გასაღების საშუალებით ყოველთვის გადადის ერთსა და იმავე შიფროტექსტში, რაც ძალიან უადვილებს კრიპტოანალიტიკოსს შიფრის გატეხვას.

ყველივე აქედან გამომდინარე, აუცილებელია, რომ (1) ფორმულის მიხედვით გამოთვლილი შიფროტექსტში თოთოეული გამოსასვლელი სიმბოლო დამოკიდებული იყოს ყველა შესასვლელ სიმბოლოზე.

ამ მიზნის მისაღწევად შემოთავაზებულია დაშიფვრის ალგორითმი, რომელიც იყენებს ჰილის ალგორითმის [7] მოდიფიკაციას.