ШЕМИ И ИГРИ ЗА ПОДЕЛБА НА ТАЈНА

Д-р Невена Серафимова [1]

[1] *Универзитет „Гоце Делчев“, Штип*

Воена академија „Михало Апостолски“, Скопје

e-mail: nevena.serafimova@gmail.com

Поделбата на тајна опфаќа методи за распределба на некоја тајна помеѓу членови на одредена група (коалиција), така што секој од нив поседува еден нејзин дел. Тајната може да се реконструира само ако доволен број на делови, кои можат да бидат од различен тип, се комбинираат заедно. Притоа, секој од индивидуалните делови нема изолирана употребна вредност. Шемите за поделба на тајна се идеални за чување на информации кои се исклучително сензитивни и важни, како на пример клучеви за шифрирање, кодови за лансирање проектили или банкарски сметки. Делењето на тајна овозможува достигнување на произволно високи нивоа на доверливост и сигурност. Ги разгледуваме двете најпознати шеми за поделба на тајна (Шамир 1979, Блејкли 1979), и презентираме нивна специфична примена во игрите „фрлање на паричка преку телефон“ и „покер преку телефон“.