KVANTNA KRIPTOGRAFIJA

- danas se računalna sigurnost zasniva na nedokazanoj činjenici da NE POSTOJI EFIKASAN ALGORITAM za faktorizaciju velikih brojeva za izračun diskretnog algoritma
- Shor, 1994.: kvantni algoritam (ostvariv na kvantnom računalu) za brzu faktorizaciju brojeva
- rješenje: QKD protokol

PROTOKOL BB84

- prvi QKD protokol
- predložili ga Charles H. Bennett (IBM) i Gilles Brassard (Montreal)
- dva kanala: javni i kvantni (optički model) >>>> SLIKA!!!
- puls polariziranog svjetla s JEDNIM fotonom
- 4 moguće polarizacije fotona :
    - baza + : foton je ili vertikalno (90°) ili horizontalno (0°) polariziran
    - baza X : foton je dijagonalno polariziran (45° ili 135°)
- sigurnost protokola temelji se na :
    - nemogućnosti kloniranja fotona
    - Heisenbergovom principu neodređenosti
- izvođenje:
    - Alice slučajno generira niz 0 i 1 i slučajni niz polarizacija i šalje Bobu (1: | i \ , 0: - i /)
    - Bob radi isto i s vjerojatnošću od 50% će pogoditi/promašiti polarizaciju
    - Alice i Bob se čuju javnim kanalom i Bob sazna od Alice koje je pogodio; ostale odbacuje; postupak se ponavlja sve dok se ne dobije dovoljno dugačak ključ
- problemi :
    - puls polariziranog svjetla s JEDNIM fotonom – ne postoji takva tehnologija danas
    - mora se ugraditi kod za ispravku pogrešaka koje se javljaju tijekom prijenosa
    - duži kabel ili veća udaljenost – veća vjerojatnost pogreške
    - 2004.g. – max. dužina kabla 60km; max. udaljenost oko 2km
    - brzina prijenosa cca 1kb/s, a treba 1Mb/s
- prvi komercijalni produkt (2002.g.)
- prva sigurna transakcija između banaka 2004.g.
- grupa prof. Antona Zeilingera na Bečkom sveučilištu je primijenila QKD protokol