

Sanly maglumatlaryň möçberiniň çalt artmagy bilen maglumat howpsuzlygynyň üpjün edilmegi häzirki zaman jemgyýetiniň önünde duran möhüm ylmy-tehniki meseleleriň birine öwrüldi. Bu ugurda kriptografiýa aýratyn ähmiýete eýe bolup, maglumatlary şifrlemek, tassyklamak we goramak boýunça ylmy taýdan esaslandyrylan usullary özünde jemleýär. Kriptografiýa diňe bir kod ýazmak däl, eýsem matematiki modelirleme, algoritmik gurluş we maglumat teoriýasy bilen berk baglanyşykly ylmy ulgamdyr.

Häzirki wagtda giňden ulanylýan simmetrik we assimetrik şifrleme algoritmleri maglumatlaryň howpsuzlygyny üpjün etmegiň esasy guraly bolup hyzmat edýär. AES, RSA, SHA ýaly algoritmler köp ýyllap dowam eden ylmy-barlaglaryň netijesinde döredilip, häzirki wagtda bank ulgamynda, döwlet maglumat ulgamlarynda, internet arkaly maglumat alyş-çalyşda we elektron söwdada giňden ulanylýar. Bu algoritmleriň ygtybarlylygy olaryň matematiki çylşyrymlylygyna, aýratyn-da uly sandyrmalar we logarifmik hasaplamalar bilen baglanyşykly meseleleriň çözütsizligine daýanýar.

Kriptografiýanyň ösüşi diňe maglumatlary goramak bilen çäklenmän, täze tehnologiýalaryň döremegine hem ýol açdy. Blokçein tehnologiýasy, elektron gol ulgamlary, sanly şahsyýetnamalar we kriptowalýutalar häzirki zaman kriptografiýasynyň amaly taýdan in möhüm ugurlarynyň biridir. Bu tehnologiýalar maglumatlaryň üýtgedilmezligini, aç-açanlygyny we ygtybarlylygyny üpjün etmek bilen, ykdysadyýetiň dürli pudaklarynda täze mümkinçilikleri döredýär.

Soňky ýyllarda kwant hasaplamalarynyň ösmegi kriptografiýa ylmynda täze tapgyry açdy. Kwant kompýuterleriniň uly hasaplaýyş kuwwaty häzirki wagtda ulanylýan käbir şifrleme usullarynyň howpsuzlygyna howp döredip biler. Şonuň üçin dünýäniň öňdebaryjy ylmy merkezlerinde kwant kriptografiýasy boýunça giň gerimli barlaglar alnyp barylýar. Bu ugur fotonlaryň fiziki häsiýetlerine esaslanyp, maglumatlary doly goramak mümkinçiligini döredýär.

Netijede, kriptografiýa häzirki zaman maglumat jemgyýetiniň durnukly işlemeginiň möhüm ylmy binýadydyr. Ol diňe tehnologiýa däl, eýsem milli howpsuzlygyň, ykdysady ösüşiň we sanly jemgyýetiň geljeginiň möhüm bölegidir. Ylmyň bu ugry geljekde hem täze mümkinçilikleri açyp, sanly giňişligiň ygtybarlylygyny üpjün etmäge dowam eder.

Arslan JANMYRADOW

Türkmenistanyň Döwlet energetika institutynyň mugallymy