AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

ÇFARË ËSHTË KRIPTOGRAFIA?

KRIPTOGRAFIA ËSHTË TEKNIKË E SIGURIMIT TË INFORMACIONIT DHE KOMUNIKIMIT PËRMES PËRDORIMIT TË KODEVE, NË MËNYRË QË VETËM ATA PERSONA PËR TË CILËT ËSHTË MENDUAR INFORMACIONI TË MUND TA KUPTOJNË DHE TA PËRPUNOJNË ATË.

Llojet e Kriptografisë

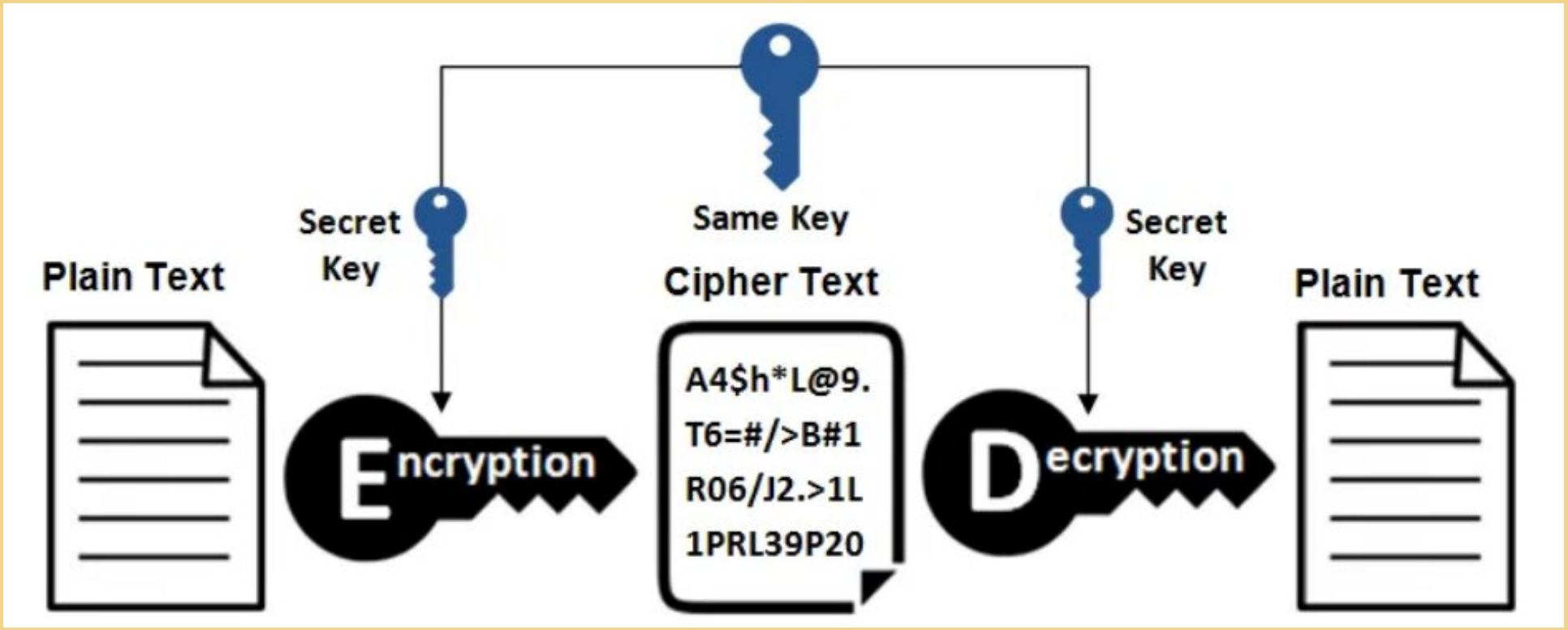
01. **Kriptografia Simetrike**

02. **Kriptografia Asimetrike**

03. **Funksionet Hash**

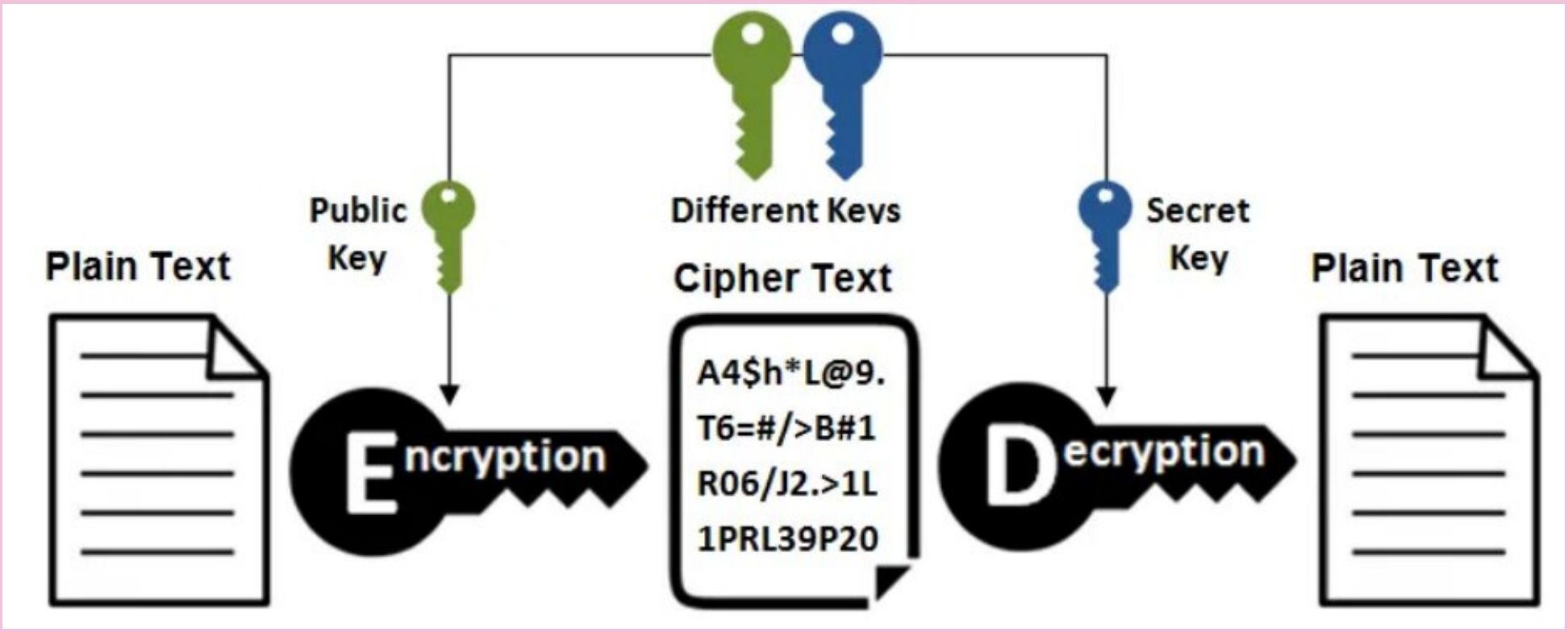
KRIPTOGRAFIA SIMETRIKE

Kriptografia simetrike mbështetet në algoritme që përdorin një çelës të vetëm për të enkriptuar dhe deshifruar informacionin. Me fjalë të tjera, dërguesi përdor një çelës sekret për të enkriptuar mesazhin. Më pas, marrësit përdorin të njëjtin çelës për të deshifruar dhe lexuar të dhënat. Pra, çelësi duhet të ndahet në të gjitha palët që janë të autorizuara për të deshifruar mesazhin.



KRIPTOGRAFIA ASIMETRIKE

Ekzistojnë dy anë në një komunikim të koduar: dërguesi, i cili kodon të dhënat dhe marrësi, i cili i deshifron ato. Duke u nisur dhe nga emri, enkriptimi asimetrik është i ndryshëm në secilën anë: dërguesi dhe marrësi përdorin dy çelësa të ndryshëm. Në këtë lloj enkriptimi të dhënat e enkriptuara me çelësin publik mund të deshifrohen vetëm me çelësin privat.



FUNKSIONET HASH

Funksionet hash janë funksione të pakthyeshme, njëkahëshe, të cilat mbrojnë të dhënat, me koston e pamundësisë për të rikuperuar mesazhin origjinal. Hashing është një mënyrë për të transformuar një varg të caktuar në një varg me gjatësi fikse. Një algoritëm i mirë hashing do të prodhojë rezultate unike për çdo hyrje të dhënë. Një hash mund të përdoret për hashimin e të dhënave (siç janë fjalëkalimet) dhe në certifikata.