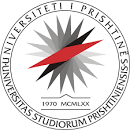
UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I SHKENCAVE MATEMATIKE-NATYRORE

Departamenti: Matematikë | Programi: Shkencë kompjuterike



Siguria e të dhënave

Asistent: Besnik Duriqi

Studentët: Alketa Hajdari dhe Elda Meshi.

**Hyrje**

**One-time pad** është një lloj teknike enkriptimi që është teorikisht i pathyeshëm. Është një metodë kriptografie me çelës simetrik që përfshin përdorimin e një çelësi të rastësishëm që është aq i gjatë sa mesazhi që është i koduar. Çelësi gjenerohet vetëm një herë dhe duhet të mbahet sekret. [1]

**Historiku**

Koncepti i OTP u propozua për herë të parë nga shkencëtari amerikan Gilbert Vernam në 1917.

Gjatë Luftës së Parë Botërore, Vernam punonte për kompaninë amerikane AT&T dhe kishte për detyrë të gjente një mënyrë për të enkriptuar me sazhet e transmetuara përmes linjave telegrafike për të parandaluar përgjimin dhe dekodimin nga spiunët gjermanë. Ai zhvilloi një sistem që përdorte një shirit kyç që përmbante një sekuencë shkronjash të rastësishme, të cilat iu shtuan mesazhit me tekst të thjeshtë për të prodhuar tekstin e shifruar. Marrësi i mesazhit do

Në vitet 1920, një tjetër shkencëtar amerikan i quajtur Joseph Mauborgne përmirësoi sistemin e Vernam duke përdorur një çelës që ishte vërtet i rastësishëm dhe jo i krijuar nga një shirit çelësi para-ekzistues. Sistemi i Mauborgne u përdor nga ushtria amerikane gjatë Luftës së Dytë Botërore dhe ishte thelbësor në sigurimin e komunikimeve të tyre kundër kodeve gjermane. Sistemi OTP fitoi përdorim të gjerë gjatë Luftës së Ftohtë, ku u përdor nga SHBA dhe Bashkimi Sovjetik për komunikim të sigurt midis agjencive të tyre të inteligjencës. Sidoqoftë, ai nuk ishte i pagabueshëm dhe kishte raste kur çelësi ishte komprometuar ose keqpërdorur, duke çuar në prishjen e kriptimit. Pavarësisht dobësive të tij, sistemi OTP mbetet një nga format më të sigurta të kriptimit nëse përdoret si duhet, pasi siguron sekret të përsosur dhe është rezistent ndaj sulmeve edhe nga kompjuterët më të fuqishëm. [3]

**Si funksionon one-time pad ?**

Gjeneroni një çelës të rastësishëm: Çelësi është një sekuencë e rastësishme karakteresh që është të paktën aq e gjatë sa mesazhi që do të kodohet.

Enkriptoni mesazhin: Për të enkriptuar mesazhin, çdo karakter i mesazhit kombinohet me një karakter përkatës nga çelësi duke përdorur shtimin modular. Për shembull, nëse mesazhi është "HELLO" dhe çelësi është "XMCKL", karakteri i parë i mesazhit të koduar do të jetë "H" + "X" = "I", karakteri i dytë do të jetë "E" + "M " = "J," dhe kështu me radhë.

Dërgo mesazhin e koduar: Mesazhi i koduar tani mund të dërgohet përmes një kanali të pasigurt.

Deshifrimi i mesazhit: Për të deshifruar mesazhin, marrësi përdor të njëjtin çelës për të kryer operacionin e kundërt. Çdo karakter i mesazhit të koduar kombinohet me karakterin përkatës nga çelësi duke përdorur zbritjen modulare. Për shembull, nëse mesazhi i koduar është "IJWYF" dhe çelësi është "XMCKL", karakteri i parë i mesazhit të deshifruar do të ishte "I" - "X" = "H", karakteri i dytë do të ishte "J" - " M" = "E" dhe kështu me radhë.Është e rëndësishme të theksohet se siguria e bllokut një herë varet nga fakti se çelësi është vërtet i rastësishëm dhe përdoret vetëm një herë. Nëse çelësi ripërdoret ose jo vërtet i rastësishëm, kriptimi mund të prishet lehtësisht. Për më tepër, çelësi duhet të shpërndahet në mënyrë të sigurt si te dërguesi ashtu edhe te marrësi përpara se çdo mesazh të mund të kodohet dhe deshifrohet [2]

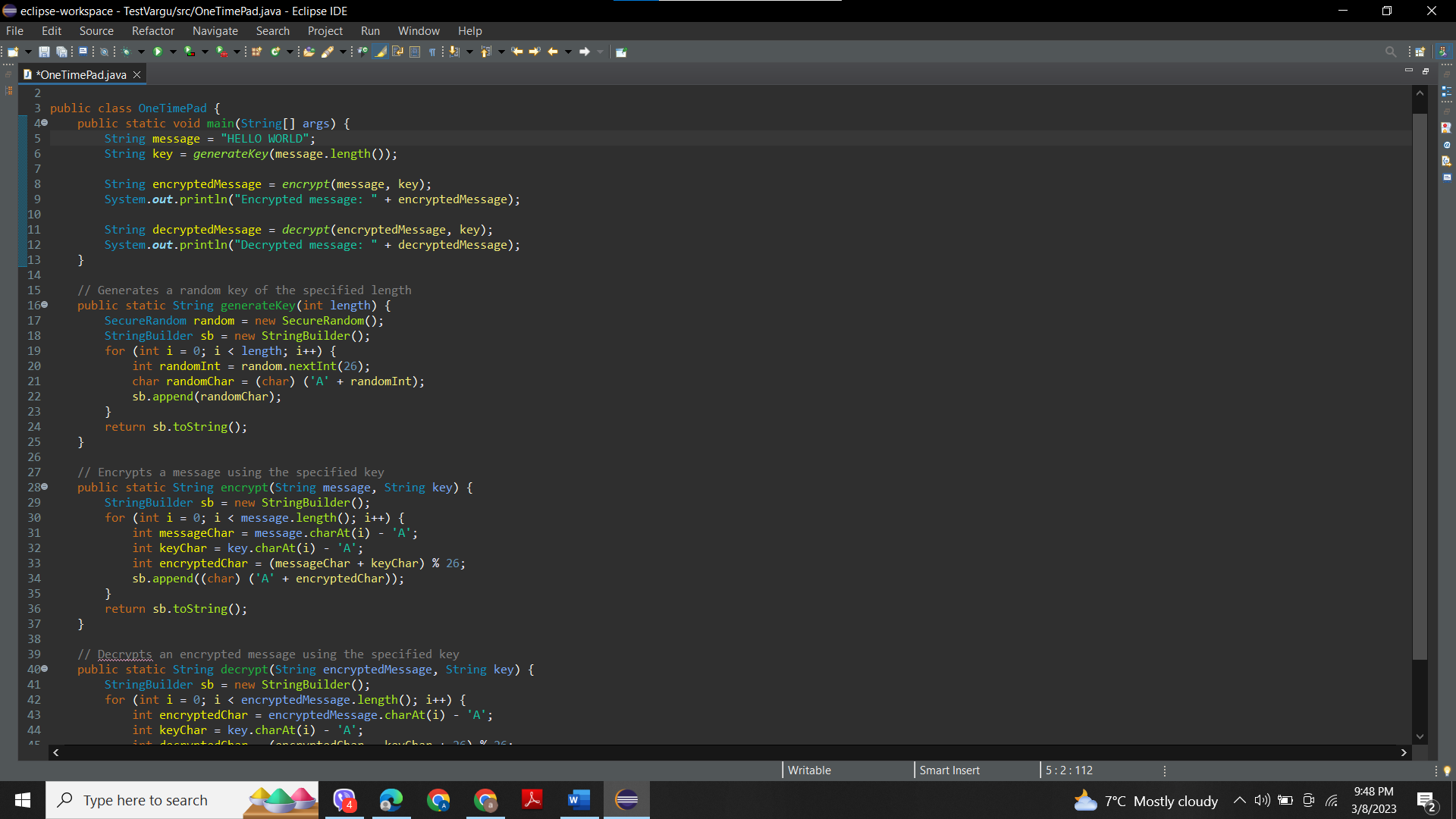
**Si perdoret one-time pad?**

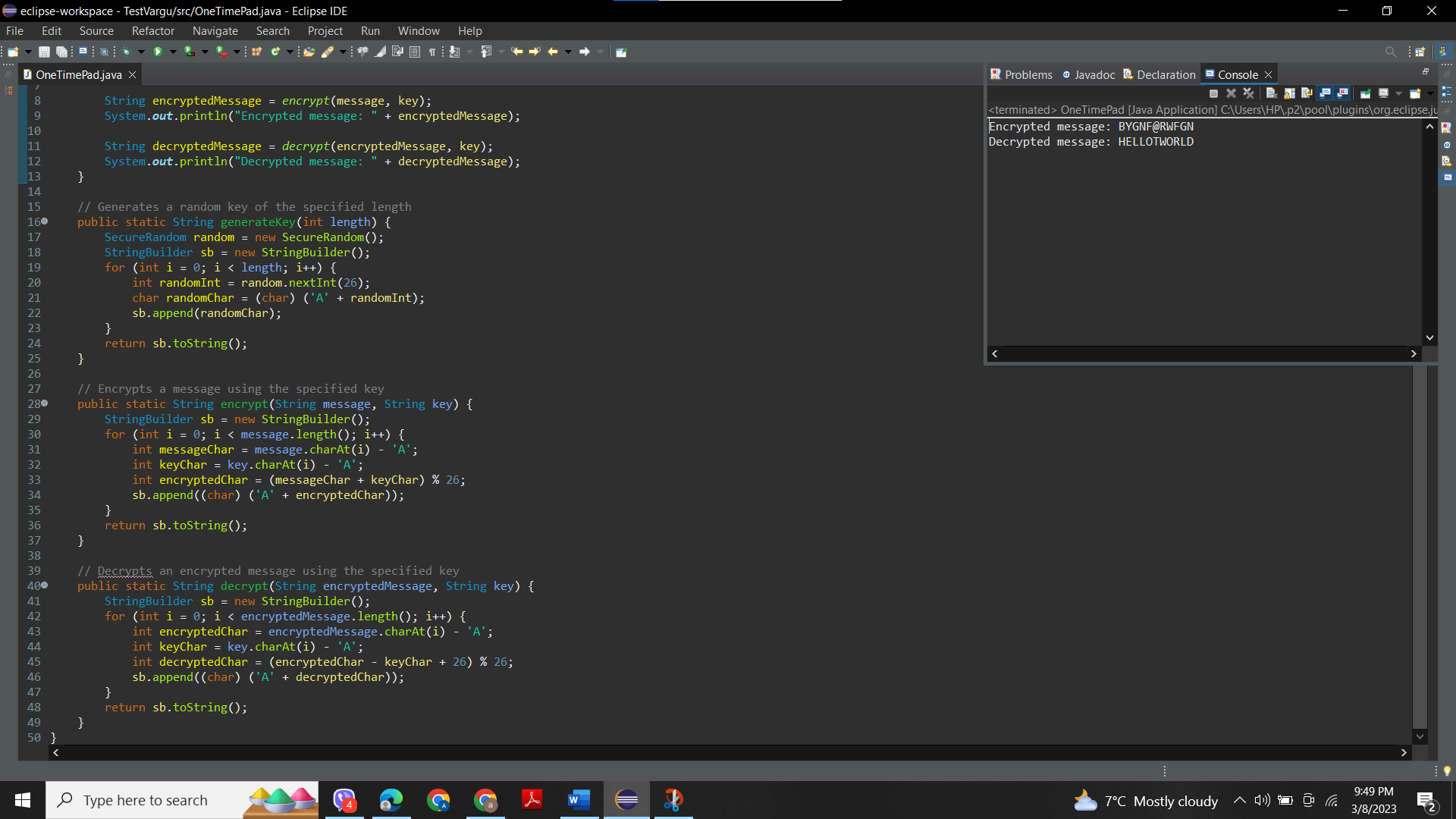
Edhe pse one-time pad është me të vërtetë e vetmja metodë e kriptimit të pathyeshme, përdorimi i tij është jopraktik për shumë aplikacione moderne, sepse sistemi duhet të plotësojë kushtet e mëposhtme:

* Çelësi duhet të jetë i njëjtë me madhësinë e mesazhit që dërgohet.
* Çelësi duhet të jetë vërtet i rastësishëm.
* Çelësat nuk duhet të ripërdoren kurrë.
* Çelësat duhet të ndahen në mënyrë të sigurt midis palëve dërguese dhe pranuese

Për shkak të këtyre kushteve të rrepta, përdorimi i bllokut një herë mbi mediat dixhitale është i pamundur. Kushtet më sfiduese qëndrojnë në gjenerimin e çelësave vërtet të rastësishëm, pamundësinë për të ripërdorur një çelës dhe ndarjen e atyre çelësave me palën marrëse. Për shkak të natyrës së shpërndarë të rrjeteve kompjuterike dhe mënyrës se si ndahen të dhënat në internetin global, mekanizmat e tjerë të enkriptimit janë më të përshtatshëm, megjithëse më pak të sigurt në praktikë. Pajisja e njëhershme është shndërruar në një metodë interesante të kriptimit që është përdorur me sukses në një epokë para teknologjisë. [4]3

Ky është një shembull i zbatimit të një kodi one-time pad ne java:





Në këtë shembull, ne fillimisht gjenerojmë një çelës të rastësishëm me të njëjtën gjatësi si mesazhi duke përdorur metodën generateKey. Më pas përdorim metodën e enkriptimit për të kriptuar mesazhin duke përdorur çelësin dhe metodën e dekriptimit për të deshifruar mesazhin e koduar duke përdorur të njëjtin çelës.

Vini re se në këtë zbatim, ne përdorim vetëm shkronja të mëdha dhe supozojmë se mesazhi dhe çelësi janë të së njëjtës gjatësi. Në praktikë, one-time pad mund të përdoret me çdo grup karakteresh dhe mesazhi dhe çelësi mund të jenë me gjatësi të ndryshme, për sa kohë që çelësi është të paktën aq i gjatë sa mesazhi.

Referencat

[1]<https://www.techtarget.com/searchsecurity/definition/one-time-pad>

[2]<https://www.cia.gov/legacy/museum/artifact/one-time-pads/#:~:text=A%20one-time%20pad%20%28OTP%29%20is%20a%20crypto%20algorithm,encoder%20and%20a%20matching%20pad%20for%20the%20decoder>

[3]<https://www.liquisearch.com/one-time_pad/history_of_invention>

[4] <https://security.stackexchange.com/questions/108682/is-one-time-pad-used-anywhere>