|  |  |
| --- | --- |
| **Fag / Navn:** Kryptering 16484 Softwaretest og sikkerhed | **Varighed:** 5 dage |
| **Fagtype:** Bundet | |
| **Uddannelse**: Datateknikker med programmering | |
| **Præsentationsstandard**: Avanceret | |
| **Beskrivelse af faget** | |
| Faget kryptering som en del af faget ”Softwaretest og sikkerhed”, som fordeles over to hovedforløb.  Som softwareudvikler har du en pligt overfor din arbejdsgiver til at sikre og beskytte deres data. I denne fag lærer du, hvordan du bruger .NET Framework til at beskytte dine data i forhold til følgende:   * Fortrolighed * Integritet * ikke-afvisning * Godkendelse   Faget vil blandt andet omhandle tilfældige talgenerations-, hashing-, autentificering hashing- og adgangskodebaserede nøgledivationsfunktioner. Vi kommer også både ind på symmetrisk og asymmetrisk kryptering ved hjælp af DES, Triple DES, AES og RSA.  Faget afsluttes med en diskussion om hvordan man kombinerer de lærte hash- og krypteringsalgoritmer sammen til produkt - et hybridkrypteringsprogram - der inkluderer AES, RSA, HMACS og Digital Signatures. | |
| **Uddannelsesmål** | |
| 10. Eleven har en generel viden om data-kryptering, og kan anvende krypteringsformer som f.eks. SSL i forbindelse med udvikling af applikationer.  11. Eleven kan indhente viden omkring softwaresikkerhedsstandarder og kendte sikkerhedshuller i eksisterende software.  12. Eleven har en generel viden om authentication og kan udvikle programmer, der anvender authentication.  13. Eleven har en generel viden om Hashing-kodning, og kan anvende kodningsformer som f.eks. MD5 i forbindelse med udvikling af applikationer.  14. Eleven har en generel viden om forskellige former for hacking angreb, som f.eks. SQL injection og XSS (Cross-Site Scripting), og kan anvende denne viden til at sikre egne udviklede webbaserede applikationer.  15. Eleven kan anvende forskellige website security tools til at teste sikkerheden på udviklet software. | |
| **Læringsmål** | |
| **Tilfældighed 10,11**  *Elever arbejder med Pseudo-tilfældige tal sikre tilfældige tal, der udvikler en generator der* genererer tilfældige tal af høj kvalitet. *Yderligere definere eleven en test på tilfældigheden af RNGCryptoServiceProvider sammenlignet med Random på store datamængder.* | |
| **Læringsmål** | |
| **HASH 13**  Hashing bruges til at sikre data-integritet af beskeder. Dvs. hashing sikrer at bliver indholdet i beskeden ændret, vil det blive opdaget. Eleven arbejder med hashing funktioner der er beskrevet i System.Security.Cryptography. Eleven udvikler en appliaktion, hvor i der kan vælges Hash- eller HMAC-algoritme, generer nøgler (i tilfælde af HMAC), hash besked og verificer (i tilfælde af HMAC) deres hashes. Grænsefalden ska vise plain text og hash både i ASCII og HEX; og den tid, der kræves af hash- og HMAC-operationerne. | |
| **Læringsmål** | |
| **Sikker adgangskodelagring 12, 13**  Eleven lære at hashing-algoritmer er en-vejs funktioner. Der forvandler enhver datamængde til et "fingeraftryk" med fast længde. Emnet omhandler også Rainbow Tables og Brute Force angreb og hvordan dette forhindres via Password Based Key Derivation samt skalering af disse.  Eleven udvikler en applikation der lager hash password plus salt over tid. Salt benyttes den udviklede tilfældighedsgenerator. Programmellet skal kunne håndterer MD5, SHA familien samt HMAC | |
| **Læringsmål** | |
| **Symmetrisk kryptering**  Eleven præsenteres for de symmetriske kryptografiske primitiver som er understøttet .NET frameworks namespace System.Security.Cryptography i henhold til DES, 3DES, AES.  Eleven udvikler et program, der giver mulighed for at vælge en symmetrisk krypterings algoritme, generer nøgler, krypter og dekrypter beskeder.  Yderligere opsamles der data om beregningsomkostningerne der kræves af DES, 3DES og AES krypterings- og dekrypteringsoperationerne. | |
| **Læringsmål** | |
| **Asymmetrisk kryptering**  **Eleven lærer om** RSA krypteringssystemet baseret på systemets udførelsesform i .NET frameworket ses i forhold private og offentlige nøgler, hvordan nøgler udveksles, impoteres og ekspoteres samt at sikkerheden i systemet hviler på antagelsen om at primtalsfaktorisering og modulær aritmetik.  Eleven udvikler programmel der skal fungere som sender og modtager af/til RSA-kommunikation. Yderligere opsamles der data om beregningsomkostningerne der kræves af DES, 3DES og AES krypterings- og dekrypteringsoperationerne | |
| **Bedømmelse** | |
| Faget bedømmes efter 7-trinsskalaen og karakteren afgives den sidste dag på hovedforløbet. Eleven evalueres individuelt ud fra afleveringer, fremlæggelser, deltagelse i undervisningen, samt afsluttende modulprojekter. | |
| ***Faget bidrager til følgende kompetencemål****: 33,34* | |