Undervisningsplan kryptering

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Uge** | **Dag** | **Emne** | **Pensum** | **Øvelse** |
| 1 | 1 | **Introduktion**  The Moodle – forløbsopbygning  **LUP**  **Hvad er kryptering**  - Fortrolighed/confidentiality  - Integritet/integrity,  - ikke-afvisning/non-repudiation,  - Godkendelse/ autentificering  - Erfaringer med kryptering  **Preforløb**  txt: The difference between Encryption, Hashing and Salting  **UV**  1 introduktion.pptx  2 Random.pptx  Demo RandomNumbers | The Moodle  Introduktion  Kryptografiske pseudo vs. sikre tilfældige tal | Tilfældigheder |
| **Hvad er Hashing**  - Algoritmer  - Virkemåde 1093 X 1039 = 1.135.627  - Envejs  **UV** 3 Hashing  Demo Hash, HMAC | The Moodle  Hashing-algoritmer  **Installation af database efter eget valg og opret forbindelse hertil igennem C#** | Opgave hashing |
| **2** | **Gennemgang af øvelser v/elev**  **Password**  - Sikkerhed  - Salt + hash  - Lagring  - PBKDF2  **UV** 4 SecurePasswordStorage Demo HashPasswords, PBKDF | The Moodle  Sikker adgangskodelagring | Sikker lagring af adgangskode |
| 3 | **Gennemgang af øvelser v/elev**  **Symmetriske algoritmer**  - Kryptering med delt nøgle  - Transposition, permutation, substitution  - DES, Triple DES og AES  UV  5 SymmetriskKryptering Demo DES, Triple DES og AES v/elev | The Moodle  Symmetrisk kryptering | Symmetrisk kryptering |
| 4 | **Gennemgang af øvelser v/elev**  Fremlæggelser  Målpind 14&15  **Asymmetriske algoritmer**  - Kryptering offentlig/privat  - Transposition, permutation, substitution  - RSA  - Hastighed | The Moodle  Asymmetrisk kryptering | Asymmetrisk kryptering |
| 5 | **Do**  **Evaluering**  Ingen karakter skal ind gå i projekt |  |  |