# DANH SÁCH MỘT SỐ CHỦ ĐỀ BTL

|  |  |  |  |
| --- | --- | --- | --- |
| TT | Nội dung | Số SV tối đa | Buổi báo cáo |
|  | Chuẩn mật mã khóa công khai trên đường cong EllipticGiới thiệuChuẩn thuật toán mật mã khóa công khai trên đường cong EllipticCài đặt |  | **Tuần 3** |
|  | Nghiên cứu bộ tạo số giả ngẫu nhiên và một số thuật toán mã dòng*(tham khảo tại các tài liệu: [1-c3], [2], [3])*Bộ tạo số giả ngẫu nhiênNhắc lại một số khái niệmĐộ đo EntropyThiết kế PNGCác thuật toán PNGMã dòngGiới thiệuMã dòng RC4Thuật toán E0 cho BluetoothHệ mã OTPThuật toán A5/1 cho GSMCài đặt |  | Tuần 3 |
|  | Nghiên cứu về hàm dẫn xuất khóa*(tham khảo tại các tài liệu: [1-c5&6], [2], [3])*Giới thiệu về hàm dẫn xuất khóaDẫn xuất khóa PKCS#5Cài đặt thực thi |  | Tuần 4 |
|  | Các giao thức thiết lập khóa*(tham khảo tại các tài liệu: [5], [6], [1], [2], [3])*Giới thiệuTruyền khóa dựa trên mã hóa khóa đối xứngThỏa thuận khóa dựa trên mật mã đối xứngTruyền khóa dựa trên mã hóa khóa công khaiThỏa thuận khóa dựa trên mật mã bất đối xứngCài đặt |  | **Tuần 4** |
|  | Ứng dụng của mật mã trong lưu trữ mật khẩu trong trình duyệt Firefox trên Windows(tham khảo tại tài liệu: [7], [8], [9])Giới thiệuCách thức lưu trữCác thành phần mật mã sử dụngPhân tích độ an toànLập trình triển khai (có thể sử dụng mã nguồn mở) |  | **Tuần 4** |
|  | Ứng dụng của mật mã trong lưu trữ mật khẩu trong trình duyệt Firefox trên Android(tham khảo tại tài liệu: [7], [8], [9])Giới thiệuCách thức lưu trữCác thành phần mật mã sử dụngPhân tích độ an toànLập trình triển khai (có thể sử dụng mã nguồn mở) |  | **Tuần 4** |
|  | Nghiên cứu và lập trình ứng dụng sử dụng thư viện OpenSSL *(tham khảo [10], [11])*   * 1. Tổng quan về OpenSSL   2. Kiến trúc OpenSSL   3. Các thành phần mật mã trong OpenSSL   4. Xây dựng ứng dụng mã hóa sử dụng thư viện OpenSSL |  | **Tuần 4** |
|  | Tìm hiểu giao thức đồng thuận Proof of Work [12]  * Blockchain * Giao thức đồng thuận * Proof of Work * Cài đặt triển khai |  | **Tuần 4** |
|  | Tìm hiểu về Zero Knowledge Proof [13]  * Tổng quan về Zero Knowledge Proof * Cơ chế hoạt động của một số giao thức Zero Knowledge Proof * Cài đặt triển khai |  | **Tuần 4** |
|  | Tìm hiểu thư viện tf-encrypted và ứng dụng [14], [15]  * Tổng quan về tf-encrypted * Kiến trúc của tf-encrypted * Các thành phần mật mã trong tf-encrypted * Cài đặt ứng dụng có sử dụng tf-encrypted |  | **Tuần 4** |
|  | Tìm hiểu thư viện PySyft và ứng dụng [16]  * Tổng quan về PySyft * Kiến trúc của PySyft * Các thành phần mật mã trong PySyft * Cài đặt ứng dụng có sử dụng PySyft |  | **Tuần 4** |
|  | Tìm hiểu về lược đồ chia sẻ bí mật (Secret Sharing Scheme) và ứng dụng [17], [18]  * Tổng quan * Xây dựng * Chia sẻ bí mật và tính toán bảo mật nhiều thành viên * Cài đặt triển khai |  | **Tuần 4** |
|  | Nghiên cứu về giải thuật mã hóa RSA  * Tổng quan * Cách thức mà RSA hoạt động * Cài đặt |  | **Tuần 4** |
|  | Nghiên cứu thuật toán 3-DES  * Kiến trúc của 3-DES * Nguyên lý và cơ sở hoạt động * Tại sao 3-DES lại phổ biến? * Cài đặt |  | **Tuần 4** |
|  | Nghiên cứu cách thức và giải thuật mã hóa an toàn với reCaptcha  * Tổng quan * Đánh giá phương thức + an toàn của reCaptcha * Cài đặt |  | **Tuần 4** |
|  | Nguyên lý số nguyên lớn áp dụng trong mật mã RSA  * Giải pháp lưu trữ số nguyên lớn * Các kiểm tra 1 số nguyên lớn là số nguyên tố |  | **Tuần 4** |

1. **Tài liệu tham khảo**:
2. St Denis, Tom. *Cryptography for developers*. Elsevier, 2006.
3. D. Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*, 2015.
4. Saiful Azad, Al-Sakib Khan Pathan. *Practical Cryptography: Algorithms and Implementations Using C++*, 2015.
5. [Pedro Franco](https://www.amazon.com/s/ref=dp_byline_sr_book_1?ie=UTF8&text=Pedro+Franco&search-alias=books&field-author=Pedro+Franco&sort=relevancerank). *Understanding Bitcoin: Cryptography, Engineering and Economics*, 2015.
6. Katz, Jonathan, et al. *Handbook of applied cryptography*. CRC press, 1996.
7. Schneier, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.
8. <https://pdfs.semanticscholar.org/a531/bfae3dc920c41dc9cc3b2d55528257823668.pdf>
9. <https://projekter.aau.dk/projekter/files/260127101/Master_Thesis_ICTE4___4SER_4_6.pdf>
10. <https://curve.carleton.ca/system/files/etd/8e5c251c-54f8-43b9-a3c0-b847b47b989a/etd_pdf/b73446ef00838b10e69d04e9f2c9921a/mccarney-passwordmanagerscomparativeevaluationdesign.pdf>
11. <https://pdfs.semanticscholar.org/940f/23dd53c66b81617e66f70799bea68e2b059a.pdf>
12. <https://www.codepool.biz/openssl-programming-tutorial>
13. <http://cryptowiki.net/index.php?title=Proof-of-work_system>
14. <http://cryptowiki.net/index.php?title=Zero-knowledge_proofs>
15. <https://github.com/tf-encrypted/tf-encrypted>
16. <https://medium.com/dropoutlabs/experimenting-with-tf-encrypted-fe37977ff03c>
17. <https://github.com/OpenMined/PySyft>
18. <https://www.cs.bgu.ac.il/~beimel/Papers/Survey.pdf>
19. <https://github.com/lovesh/secret-sharing-schemes>