# DANH SÁCH MỘT SỐ CHỦ ĐỀ BTL

|  |  |  |
| --- | --- | --- |
| TT | Nội dung | Ghi chú |
|  | 1. 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 BluetoothCài đặt | 1.Phạm Duy 2.Bùi Tiến Dũng  3.Dư Minh Quý  4.Nguyễn Dương Tấn Anh |
|  | 2. 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 thiệuHệ mã OTPThuật toán A5/1 cho GSMCài đặt | 1.Đỗ Thanh Phát  2.Trình Kim Chi  3.Trần Thanh Thiện  4.Nguyễn Thanh Thảo  5.Lương Thị Xuân |
|  | Nghiên cứu chuẩn mã dữ liệu tiên tiến AES*(tham khảo tại các tài liệu: [1-c4&7], [2], [3])*Giới thiệuThiết kế của AESMột số phương pháp thực thi hiệu quảCác chế độ hoạt độngChế độ mã hóa có xác thực | 1.Bùi Xuân Khải  2.Nguyễn Thế Kiệt  3.Ngô Huỳnh Thảo Phương  4.Hồ Nguyễn Tường Vi  5.Võ Văn Quý 6.Nguyễn Thành Công |
|  | 1. **Nghiên cứu về hàm băm**  *(tham khảo tại các tài liệu: [1-c5&6], [2], [3])*Giới thiệuThiết kế và thực thi họ hàm băm SHSCài đặt | 1.Nguyễn Thị Xuân Lan  2.Diệp Hân  3.Trần Hữu Anh Văn  4.Nguyễn Trần Anh Hoàng  5.Kiều Tấn Dương |
|  | Nghiên cứu mã xác thực thông điệp*(tham khảo tại các tài liệu: [1-c5&6], [2], [3])*Giới thiệuMã xác thực thông điệp dựa trên hệ mậtMã xác thực thông điệp dựa trên hàm bămCài đặt | 1.Võ Thị Kiều Trinh  2.Nguyễn Phan Thanh Sang  3.Trần Hoàng Hiệp  4.Phan Trí Vy |
|  | 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 | 1.Nguyễn Công Thạnh  2.Phan Trần Xuân Nghĩa  3.Thái Tường An  4.Lưu Văn Lân  5.Nguyễn Tấn Phát  6.Lê Nguyễn Hoàng Anh Nhớ |
|  | Chuẩn mã hóa khóa công khai RSA*(tham khảo tại các tài liệu: [1-c9], [2], [3])*Giới thiệuChuẩn thuật toán mật mã khóa công khai RSACài đặt | 1.Hồ Thiên Kim  2.Lê Đức Nhớ  3.Hoàng Quốc Cường  4.Nguyễn Văn Tâm  5. Nguyễn Văn Nhân |
|  | Chuẩn ký số RSA*(tham khảo tại các tài liệu: [1-c9], [2], [3])*8.1. Giới thiệu8.2. Chuẩn thuật toán ký số RSA8.3. Cài đặt | 1.Phan Duy Cường  2.Lều Thị Hoài  3.Vũ Thị Thủy Tiên  4.Lê Tú Trinh |
|  | 9. Chuẩn mật mã khóa công khai trên đường cong EllipticGiới thiệu9.2. Chuẩn thuật toán mật mã khóa công khai trên đường cong Elliptic9.3. Cài đặt | 1.Phan Nguyễn Hiếu Vinh  2.Phạm Văn Xuất  3.Phạm Trần Sang  4.Trần Minh Hòa  5.Phạm Thảo Hiền  6.Huỳnh Phương Nam |
|  | Các giao thức thiết lập khóa*(tham khảo tại các tài liệu: [5], [6], [1], [2], [3])*10.1. Giới thiệu10.2. Truyền khóa dựa trên mã hóa khóa đối xứng10.3. Thỏa thuận khóa dựa trên mật mã đối xứng10.4. Truyền khóa dựa trên mã hóa khóa công khai10.5. Thỏa thuận khóa dựa trên mật mã bất đối xứng. Cài đặt | 1.Phạm Thương Mến  2.Thiều Thùy Trang Nữ  3.Trần Võ Anh Thư  4.Nguyễn Văn Minh Hoàng  5.Phan Văn Sự |

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.