Criptografie și securitate CTI

Laborator 8

Criptosisteme cu cheie publică. Textbook RSA

1. (a) Fie $p = 43$ și $q = 23$ factorii unui modul RSA. Care dintre $e_1 = 6$, $e_2 = 17$, $e_3 = 157$ este un exponent de cifrare valid?
   (b) Fie criptosistemul RSA cu $p = 31, q = 37$ și $e = 17$ (exponentul de criptare). Determinați exponentul de decriptare d.

2. (a) Folosind link-ul următor factorizați următorul modul RSA de 128 de biți:
   $n = 234841136411758273000763594354834942653$.
   `https://www.alpertron.com.ar/ECM.HTM`
   (b) Determinați valoarea exponentului de decriptare d știind că $e = 65537$.
   (c) Folosind valoare d determinată anterior, decriptați ciphertext-ul interceptat $c = 85145455636861892720413552342581283108$. Transformați pe rând rezultatul în format hex și după în ASCII.
   `https://www.dcode.fr/modular-exponentiation`

3. Generați chei RSA folosind OpenSSL urmărind pașii de mai jos:
   (a) Folosind OpenSSL, generați pentru Alice o cheie RSA pe 2048 biți, stocată într-un fișier *alice_sk.pem*.
   (b) Care este valoarea exponentului de criptare?
   (c) Decodați această cheie. Aflați valoarea modulului N și a celor două numere prime p și q.
   (d) Cheia lui Alice nu este protejată în niciun fel, deci este vulnerabilă. Alegeți o parolă puternică și generați o nouă cheie protejată folosind această parolă și AES256.
   (e) Ce diferențe observați? Decodați această cheie folosind parola folosită la creare.
   (f) Care este valoarea exponentului de criptare? Ce observați? Impactează această alegere securitatea?
   (g) Exportați cheia publică a lui Alice în fișierul *alice_pk.pem*. Decodați această cheie pentru a vedea valorile modulului și exponentului.
   `https://www.openssl.org/docs/man1.1.1/man1/openssl-smime.html`

4. Realizați criptarea hibridă urmărind următorii pași

(a) Jucați rolul lui Bob. Criptați fișierul *bob_message.txt* folosind RSA și cheia generată anterior. Încercați să criptați fișierul *bob_message.rtf* folosind RSA și cheia generată anterior. Ce observați? De ce se întâmplă aceasta?

`https://www.openssl.org/docs/man1.1.1/man1/openssl-pkeyutl.html`

(b) Folosiți criptarea hibridă pentru a cripta mesajul lui Bob către Alice. Pentru aceasta, generați o cheie simetrică pe 256 biți (32 bytes) și folosiți această cheie pentru criptarea fișierului *bob_message.rtf* cu AES-CTR. Criptați noua cheie asimetric, folosind RSA.

`https://www.openssl.org/docs/man3.0/man1/openssl-enc.html`

(c) Jucați rolul lui Alice. Folosiți fișierele criptate primite (criptarea cheii AES folosind RSA și criptarea mesajului folosind AES-CTR), decriptați și obțineți mesajul inițial.

5. Verificați certificatul digital al facultății urmărind pașii de mai jos:

(a) Cine a emis certificatul digital?

(b) Care este validitatea certificatului?

(c) Pe câți biți este definită cheia publică?

(d) Care este valoarea exponenților de criptare din certificat și din certificatele care îl atestă în lanț? Ce observați? Are aceasta impact asupra securității?