

Zadanie 5

Podać przykład systemu kryptograficznego RSA dla $n=11*13$ i podać przykład szyfrowania i deszyfrowania tym szyfrem.

Szyfr z kluczem niesymetrycznym, czyli mamy klucz publiczny i klucz prywatny.

Krok 1: wybranie liczb p i q , oraz małej liczby $e=10$ -12 bitów losowe względnie pierwsze.

obliczamy $n=p*q$;

obliczamy $\phi(n) = \phi((p-1)(q-1)) = (p-1)*(q-1)$;

$\phi(n)$ - jest elementem prywatnym; a n publicznym;

Krok 2: klucz publiczny to n oraz e

Krok 3: obliczenie $d=e^{-1} \pmod{\phi(n)}$ - klucza prywatnego.

Krok 4: obliczenie szyfrogramu: $C=m^e \pmod{n}$; gdzie m - tekst jawny, C szyfrowany;

Krok 5: odszyfrowanie: $m=C^d \pmod{n}$

Zadanie 6

Pokazać, że w systemie kryptograficznym RSA rozkład liczby n na czynniki pierwsze łamie RSA.

klucz publiczny to znane n (oraz e);

klucz prywatny wymaga znajomości $\phi(n)$; a to można wyliczyć $\rightarrow \phi(n) = \phi(a*b) = \phi((p-1)(q-1))$;

jeśli znamy rozkład n na a i b to wyliczymy $\phi(n)$;

dalej policzymy $d=e^{-1} \pmod{\phi(n)}$;

a d jest kluczem prywatnym.

Zatem bezpieczeństwo klucza prywatnego polega na trydności znalezienia a i b (lub p i q)

Zadanie 7

Podać przykład systemu kryptograficznego Rabina dla $n=13*17$ i podać przykład szyfrowania i deszyfrowania tym szyfrem.

niech $n=p*q$ gdzie $p=3 \pmod{4}$ i $q=3 \pmod{4}$;

funkcja Rabina $f(x) = x^2 \pmod{n}$ i jest podobna do szyfru RSA przy wybraniu liczby $e=2$

szyfrowanie $C = m^e \pmod{n}$

deszyfrowanie $m=C^d \pmod{n}$ gdzie $d=e^{-1} \pmod{\phi(n)}$

Zadanie 8

Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od 10^{-100}

pojedyncza runda powtórzona k razy zapewnia, że prawdopodobieństwo fałszywego uwierzytelnienia nie przekracza 2^{-k} razy.

a zatem ponieważ $10 < 2*2*2*2$ to:

$$(2*2*2*2)^{-100} = 2^{-103}$$

zatem musimy zastosować $k=103$ rundy.

Zadanie 9

Wykorzystując bibliotekę Open SSL napisać skrypt szyfrujący szyfrem AES i skrypt deszyfrujący szyfrem AES (w trybach CBC, CFB, ECB, OFB). Podać przykłady szyfrowania dla różnych plików i kluczy.

```
Rsa4096 rsa = new Rsa4096( "C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\OpenS-  
SL\\private_key_rsa_4096_pkcs8-generated.pem", "C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\  
OpenSSL\\public_key_rsa_4096_pkcs8-exported.pem" );  
  
String expected = getFileAsString("C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\  
OpenSSL\\file_unencrypted.txt");  
String encryptedAndEncoded = getFileAsString("C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\  
CodeInJava\\OpenSSL\\file_encrypted_and_encoded.txt");  
  
System.out.println( rsa.encryptToBase64(expected) );  
//String actual = rsa.decryptFromBase64( encryptedAndEncoded );  
}
```

// crypted:

```
Y60tZhMXQh92BQ867kqHDaDSHcvw90s++zovApSutZrDXd3W3K00z6bPs4J7hUIGGKAJ4kkpDDGyyIBRSaYHwwU+e08UoYoFui-  
FRyV3pi95Eyg2rlyHawvQZ5zx6LjMCbtCPeCVT0vBR2LZNCcIvS+19gb5R1WgcnhFRq303em2QAFII0c9CwPrCG6059fCYtnZuy-  
cdOuUoQ0LYex+XKKL4N5lH0n+9e96LR9YBqt25jPaWmoMWiW5kVzmN4ZbP8Dc4GJJWz7IVgsZMZzvKN4B+8K/LoEBieehVQgS/  
TGKSbwEEuG2uh20Q4Jq7vx15wZXmBQtpDum5ul0YrunHP1yubqYZ2m9ul9qZ4GJiFccxOPkt57hQJ8AndL1wDQ3I56/bMwEmJ94CyL+iA2NIr8ZCTQ-  
JF06KHaeH7wsQzzinu9YTk7+4nmF4nCw31U1EFE9Gxp0GI+Xe++tDXLK3pQx0c2Uahn/X793jhcGM1234RCqRq5RRF+ibuUeFHMIR+OL4VjqyYZD-  
15KZ/51BTiNdnX+SAoDbUaPVJhrk7rXGIl1kFSPpPM3vGLKAaBR5deg99/6ghA2bviu+Ja0q5h59Y/NKTzb2iIAev344b+jpjcVGqaxAD/DvkC-  
M05MSVJ06I4U7fFvVfogu4dgR5T+hQYgbGp+cG2sMLpiszdx/w=
```

Zadanie 10

Pokazać, że jeśli $\text{NWD}(a,m)=1$ (gdzie $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \geq 2$) to dla dowolnego $n \in \mathbb{Z}$

$$a^n \equiv a^{[n]} \pmod{m} \text{ - równoważne z pierścieniem } \mathbb{Z}_m$$

Krótko, ale niezbyt jasno:

„jeśli podstawa potęgi i m są względnie pierwsze to na wykładnikach pracujemy modulo $\varphi(m)$ ”.

jeśli podstawy a i m względnie pierwsze w pierścieniu to ich wymnożenie da jakieś “przesunięcie” b pomnożenie tego przesunięcia o $b^*m \pmod{m}=b$

a zatem oczywiste że

jeśli $a^n = b \pmod{m}$

to $b^*m \pmod{m} = b$;