Home Assignment 1

Startad: 30 mar kl 13.03

Instruktioner för Quiz

Quiz about cryptography and hashing.

Fråga 1 — 1 poäng

Compute the multiplicative inverse of 5 in $\mathbf{Z}_{21}$.

Fråga 2 — 1 poäng

Eve has an antenna that can pick up Alice's encrypted cell phone conversations. What type of attack is Eve employing?

- chosen-ciphertext attack
- chosen-plaintext attack
- ciphertext-only attack
- known-plaintext attack

Fråga 3 — 1 poäng

What is 7^{16} mod 11?

Calculation by hand!

Fråga 4 — 1 poäng

What are the next three numbers in the pseudo-random number generator $3\ x_i + 2$ mod 11, starting from $x_i = 5$?

Fill in the numbers: , , ,

Fråga 5 — 1 poäng

Why can't Bob use the pair (1,*n*) as an RSA public key, even if $n=pq$, for two large primes, p and q?

- [ ] $e=1 \Rightarrow d=e$

- [ ] 1 is a factor in *n*
- [ ] 1 doesn't encrypt the message
- [ ] 1 is not a prime

Fråga 6

1 poäng

Roughly how many times would you have to call a primality tester to find a prime number between 1,000,000 and 2,000,000? Answer with the closest integer.

Fråga 7

1 poäng

Assume that the Hill cipher matrix K is

$$K = \begin{pmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{pmatrix} K = \begin{pmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{pmatrix}$$

What is the CAT cipher?

Fråga 8

1 poäng

What is 7^{120} mod 143?

Calculation by hand!

Fråga 9

1 poäng

What are the substitutions for the following (decimal) numbers using the S-box from Figure 3 (Goodrich-Tamassia, Introduction to Computer Security, page 392)?

Substitution for 12:

Substitution for 7:

Substitution for 2:

Fråga 10

1 poäng

Show the result of encrypting M=4 using the public key (e,n)=(3,77) in the RSA crypto system.

Fråga 11

1 poäng

Assume that the Hill cipher matrix K is

$$K = \begin{pmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{pmatrix} K = \begin{pmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{pmatrix}$$

Derive the decryption matrix K^{-1}. Fill in the matrix below:

Fråga 12

1 poäng

What is the Hill cipher binary matrix K that corresponds to the permutation cipher

π:(1,2,3,4,5,6,7,8) → (2,6,8,1,3,7,5,4)?

For each row in the matrix, type in eight bits (0 or 1). No spaces or other separators! For example: 00100000

Row 1:

Row 2:

Row 3:

Row 4:

Row 5:

Row 6:

Row 7:

Row 8:

Fråga 13

1 poäng

AES supports keys of three different lengths.

Give the key lengths in increasing order (shortest key first). For each key length, write down how many different key values there are. Give the answer in exponential notation with two significant digits. For instance, 27,291,235 would be written as 2.7E7.

Length: Number of keys:

Length: Number of keys:

Length: Number of keys:

Fråga 14

1 poäng

What is the encryption of the string THELAZYFOX using the Caesar cipher (with three shift steps)?

Fråga 15

1 poäng

Show the result of an Elgamal encryption of the message M=8 using k=4 for the public key (p,g,y)=(59,2,25):

(,)

Fråga 16

1 poäng

An attacker has an encrypted message and knows the plain text is in ASCII-form. The attacker is aware of the encryption algorithm and that the key is 128 bit long. In a brute-force attack, what is the minimum number of characters of the plain-text in order to be able to find the secret key?

Fråga 17

1 poäng

Explain why non-forgeability and non-mutability imply non-deniability for digital signatures.

HTML-redigerare

Non-mutability implies non-repudiation which makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message. Non-mutability means that it's not possible to reuse a signature from a previous message.

Non-forgeability means it's not possible to counterfeit a signature. I.e. only the valid user can sign with the valid signature.

If both non-mutability and non-forgeability holds the signature cannot be denied.

p

114 ord

Fråga 18

1 poäng

Explain the strengths and weaknesses of using symmetric encryption, like AES, versus a public-key cryptosystem, like RSA.

HTML-redigerare

Symmetric cryptography primary purpose is to encrypt data and allow decryption by anyone that has the knowledge of the encrypting key.

Pros

- **Simple:** Easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages. Single-key encryption does not require a lot of computer resources when compared to public key encryption. Symmetric key encryption is much faster than asymmetric key encryption.

p

259 ord

Quiz sparad kl. 13.42

Lämna in quiz

Processing math: 100%