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 | |
| | chosen-plaintext attackciphertext-only attack | |

| Fråga 3 | 1 poäng |
|--|---------|
| What is 7 ¹⁶ mod 11? | |
| Calculation by hand! | |
| | |
| | |
| | |
| Fråga 4 | 1 poäng |
| , | |
| Fråga 5 | 1 poäng |
| | |
| Why can't Bob use the pair $(1,n)$ if $n=pq$, for two large primes, p and | |

| ☐ 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.

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 |
| Fråga 9 | 1 poä |
| | المستور (ما |
| What are the substitutions for the fo | Mowing (docimal) |
| | , |
| numbers using the S-box from Figu Tamassia, Introduction to Computer | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer | re 3 (Goodrich- |
| numbers using the S-box from Figu | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer Substitution for 12: | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer Substitution for 12: | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer Substitution for 12: Substitution for 7: | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer Substitution for 12: Substitution for 7: | re 3 (Goodrich- |
| numbers using the S-box from Figural Tamassia, Introduction to Computer Substitution for 12: Substitution for 7: | re 3 (Goodrich- |

| Show the result of encrypting $M=(e,n)=(3,77)$ in the RSA crypto sy | • |
|---|---|
| | |

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:

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

$$\pi:(1,2,3,4,5,6,7,8) \rightarrow (2,6,8,1,3,7,5,4)$$
?

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

| Row 1: | |
|--------|--|
|--------|--|

| Fraga 13 | 1 poang |
|--|---|
| AES supports keys | of three different lengths. |
| For each key length, values there are. Given | in increasing order (shortest key first). write down how many different key the answer in exponential notation digits. For instance, 27,291,235 would |
| Length: | Number of keys: |
| Length: | Number of keys: |
| Length: | Number of keys: |
| | |
| Fråga 14 | 1 poäng |
| What is the encryptic | on of the string THELAZYFOX using the |

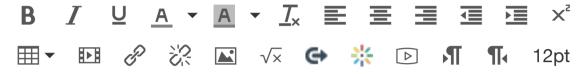
Caesar cipher (with three shift steps)?

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.

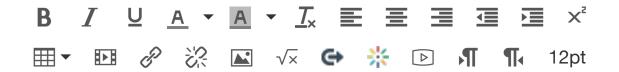
p 114 ord

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%