UNIVERSITETET I BERGEN

KANDIDAT

141

PRØVE

INF143A 0 Anvendt kryptografi

Emnekode	INF143A
Vurderingsform	Skriftlig eksamen
Starttid	31.05.2022 07:00
Sluttid	31.05.2022 10:00
Sensurfrist	--
PDF opprettet	14.05.2023 11:36

Information about the exam

Oppgave	Tittel	Oppgavetype
i	General info about digital campus exam - INF143A	Informasjon eller ressurser

General

Oppgave	Tittel	Oppgavetype
1	Basic notions	Langsvar

Classic ciphers

Oppgave	Tittel	Oppgavetype
2	Vigenere definition	Langsvar
3	Vigenere computation	Langsvar

LFSR's

Oppgave	Tittel	Oppgavetype
4	Primitive polynomials	Langsvar
5	LFSRs	Langsvar

Block ciphers

Oppgave	Tittel	Oppgavetype
6	Feistel networks	Langsvar
7	Modes of operation	Langsvar

Finite fields

Oppgave	Tittel	Oppgavetype

8	Finite fields	Langsvar

Boolean functions

Oppgave	Tittel	Oppgavetype
9	Differential uniformity	Langsvar

Asymmetric cryptography

Oppgave	Tittel	Oppgavetype
10	DHKE	Langsvar
11	DHKE computation	Langsvar
12	DHKE (other)	Langsvar

Hash functions

Oppgave	Tittel	Oppgavetype
13	Hash functions	Langsvar

1 Basic notions

Explain the difference between, and the greatest advantages and disadvantages of the alternatives in each of the following pairs:

- symmetric vs. asymmetric cryptography;
- stream ciphers vs. block ciphers.

Fill in your answer here

The advantages of using an asymmetric cipher is that its string and it can convey secure information without previously communication with that party. The downside is that asymmetric ciphers take a long time to calculate because of its reliance on modular arithmetic. So this is used to make up for symmetric ciphers weakness which is it needs some agreed apon keys to use for the cipher. The upside to symmetric ciphers is that it is much, much faster than asymmetric ones.

The advantages for using block ciphers instead of stream ciphers is that each bit in the block cipher can depend on eachother. In addition stream cipher keys will most likely be smaller than the actual message, which means the key loops around and is used multiple times. And if you send a long enough message this key kan be found. But on the other hand stream ciphers are much faster to compute because of its linearity, unlike block ciphers.

Ord: 160

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

2 5 5 5 2 5 1

2 Vigenere definition

Briefly describe how the Vigenere cipher operates on a plaintext written in the English alphabet:

- what is the key?
- how do you encrypt an English language text?
- how do you decrypt the ciphertext?

Fill in your answer here

So the Vigenere cipher is basically multiple ceasar cipher put together. So the key in this cipher is a sequence of numbers between 0 and 25 (for the english alphabet). So the key could be "1 6 12". Then when you encrypt you do it letter by letter, and shift your plaintext letter i K_i amount times to the right. Where i is your letter and K_i is the number corresponding to the letter. And if you get to the end of the key you just loop.

So for example if our key is "1 2 3" and our text is "H E L L O" we shift H 1 to the right, E 2 to the right L 3 to the right, (then we loop), so the second L shifts 1 to the right.

Now to decrypt the cipher you go through the same process as described above, the only diffrence is that you shit to the left. You dont revert any other process. So in our examle you would start to shift the first letter in the ciphertext "F" 1 posistion to the left.

Ord: 186

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

3 2 5 4 8 1 3

3 Vigenere computation

Using the Vigenere cipher with key "3-7-1-5", decrypt the ciphertext

K L B W G T F Q R K J J V H S J V D F J W.

You should get the start of quote by John Keats.

You can use the following table table giving the position of every letter in the English alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fill in your answer here

H E A R D N E L O D I E S A R D S W E E T

Ord: 21

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

8 7 5 5 6 1 4

4 Primitive polynomials

- What is the relationship between LFSR's and primitive polynomials?
- What is the relationship between primitive and irreducible polynomials?
- Give an example of a polynomial that is not primitive.

Fill in your answer here

The relasions between a LFSR and primitive polynomials is that if you want to have the most amount of security for your LFSR you need to make sure its characteristic polynomial is primitve. This is beacuse if its not primitve the LFSR can loop pre maturley which means its security level is that of a n amount of bits lower than your actual amount of bits in the LFSR.

The relations between primitive and irreducible polynomials is that a primitive polynomial is always an irreducible one, but an irreducible polynomial isn't hallways a primitive one.

(Disclaimer: I assume that this polynomial is int the finite field of F_2)

So to construct a polynomial that is not primitive we just have to construct a polynomial that isn't irreducible ether. To do this i just set in x as 0 and 1 and checks if the answers becomes 0. And if its 0 it means that the polynomial has roots, which means its not irreducible, which again means its not primitive.

$f(x) = x^4 + x^2$

$f(0) = 0^4 + 0^2 = 0$

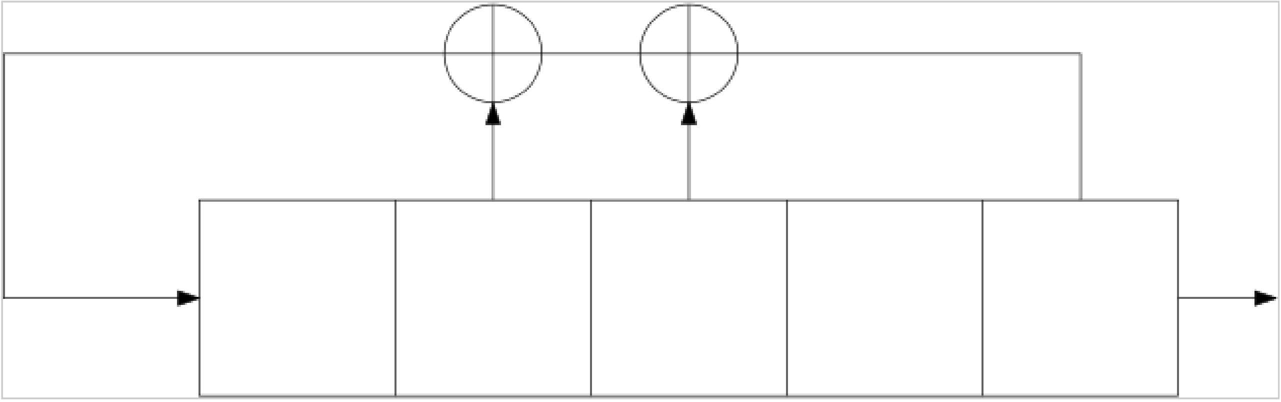
Which means it has roots

Ord: 186

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

4 9 9 9 5 1 5

5 LFSRs



Consider the LFSR given in the diagram.

- Give the recurrence relation that it represents.
- Give the characteristic polynomial.
- Simulate the LFSR with initial state (1,0,1,0,0) until it loops.
- What can you say about its characteristic polynomial?

Fill in your answer here

The recurrence relation that it represents looks as follows: S_5 = S_3 XOR S_2 XOR S_0

And its characteristic polynomials is: f(x) = x^5 + x^3 + x^2 + 1

So to simulate the LFSR we don't care about the output bit and just XOR bit nr 0, 2 and 3 counting from the right.

So we start with:

10100

then we continue with

11010

11101

11110

01111

10111

01011

00101

00010

00001

10000

01000

10100

11010

And here we see that we have looped. We didnt get what we started on which was 10100, insted we got 11010 which is the state after our intial. So from loopting through the LFSR i can say that f(x) is not a primitive polynomial since we didn't loop through all of the possible states, excluding the 0 state

Ord: 136

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

1915474

6 Feistel networks

- Briefly describe a single round of a Feistel network.
- The DES cipher (based on a Feistel network) is not considered secure anymore. What is its main weakness?
- A variant of DES called 3DES is used in which encryption with DES is performed three times (with three separate keys). Why is using only two iterations of DES not enough?

Fill in your answer here

A single round of a Feistel Network goes as follows:

* Split your text into two halves. L_i and R_i where L_i is the left part of your text, and R_i is the right part of your text

* Take R_i and set it as your L_i+1 where L_i+1 is the left part of the output of this round

* Take R_i and put it into a function F together with K_i where K_i is the round key

* Take L_i and XOR it with the output of the function F

* Then take the output of the XOR and put it as your R_i+1 where R_i+1 is the right part of the output of this round

DES's main weakness is that the length of the key is to short. When it was first introduced it was a sufficient key length , but as times evolved, machines got faster and cracking the key using brute force was now a viable option.

The reason why two iterations of DES is not sufficient is because of the meet in the middle attack. So if we have a know plain text we have the cipher text we just compute a list of all possible keys and its outcome on the first DES, then we run the second DES where we decrypt the ciphertext and see if our input text to the second DES exsists in the table we created. Now this 2DES, if you can call it that, only has a security level of 2^56+2^56 = 2^57 bits

Ord: 255

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

9634466

7 Modes of operation

Explain what modes of operation are, and why they are necessary.

Describe the ECB mode of operation. What are some of its major problems?

Describe a different mode of operation that does not have those problems.

Fill in your answer here

Modes of operation are necessary to make sure that each block of the plaintext gets sent securely

The ECB mode of operation encrypt itself block for block, so in other word we first take the plain text to the first block encrypt it using the key and we get the cipher block ,then the next block takes the next block and encrypt that block using its key. So none of the blocks rely on each other, now this a major problem because this means that the same block will always encrypt to the same cipher block no matter what the other blocks are.

A different mode of operation is CBC. In this mode you start with XORing your plaintext with an IV before you encrypt, the when encrypting the block you get C_i, the you use this C_i and XOR it with the plaintext of the second block before encrypting it to become C_i+1. Now using this we can see that CBC makes it so that every block that comes depends on every other block that comes before it.

Ord: 179

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

8 0 8 2 0 7 5

8 Finite fields

Consider the finite field $\mathbb{F}_{2^5}$constructed using the primitive polynomial $f(x) = x^5 + x^2 + 1$. Let $a = (0, 1, 1, 0, 0)$ and $b = (1, 1, 1, 0, 0)$ be two elements from $\mathbb{F}_{2^5}$.

Compute:

- $a + b$;
- $a \times b$;
- a^3.

Fill in your answer here

a + b is just XOR so:

(0,1,1,0,0) + (1,1,1,0,0) = (1,0,0,0,0)

a x b is a little bit more complicated where we will need to use f(x)

f(x) = 0

(Diclamer: this "a" is alfa)

a^5 = a^2 + 1

(0,1,1,0,0)x(1,1,1,0,0) can also be written as:

(a^3+a^2)x(a^4+a^3+a^2)

=(a^7+a^6+a^5)x(a^6+a^5+a^4)

=(((a^2+1)xa^2)+((a^2+1)+a^1)+(a^2+1))+(((a^2+1)+a^1)+(a^2+1)+a^4)

=a^4+a^2+a^3+a+a^2+1+a^3+1+a^2+1+a^4

=a^2+a+1

=(0,0,1,1,1)

and we do the same for the last problem

(0,1,1,0,0)x(0,1,1,0,0)x(0,1,1,0,0)

= (a^3+a^2)(a^3+a^2)(a^3+a^2)

= (a^6+a^5+a^5+a^4)(a^3+a^2)

= (a^3+a+a^2+1+a^2+1+a^4)(a^3+a^2)

= (a^4+a^3+a)(a^3+a^2)

= a^7+a^6+a^6+a^5+a^4+a^3

= (a^2+1)(a^2)+a^2+1+a^4+a^3

= a^3+1

=(0,1,0,0,1)

Ord: 78

Knytte håndtegninger til denne oppgaven?

Bruk følgende kode:

2 3 5 4 0 8 9

9 Differential uniformity

Define the following notions:

- (n,m)-function;
- differential uniformity.

Give pseudocode showing how the differential uniformity can be computed.

Why is differential uniformity important?

What is its optimal value?

Fill in your answer here

```
input = [];
result = [];
for i in input:
    m = compute nmfunction(i)
    result.add(difference(i, m)
```

Now here we have a list of all the differences in output and input to the mn function.
Then we can find the value that occurs the oftest in this list

Differential uniformity is important because this if its not, an attacker can analyze the difference between two inputs to gain knowledge over what the original message was.
Its optimal value is m / 2.

Ord: 81

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

2 6 5 5 3 5 4

10 DHKE

Describe the set-up and operation of the Diffie-Hellman key exchange (DHKE).

Fill in your answer here

So for the setup each part that takes part in the key exchange needs its private key. This we can sett to "a" for one person and "b" for the other person. The we have som public parameters "g" and "n" where "g" is relatively low" and "n" is relatively high. Then each part takes their private key and "g" and makes an exponent out of it then modulates it with "n". So say for example that Alice makes g^a (mod n) and Bob makes g^b (mod n) then they send this number to each other. Then when they have eachothers numbers they add their own private keys to the mix and they get a shared private key. So mathematically, for Alice, this would look like this: (g^b)^a (mod n)

Ord: 130

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

5 1 1 9 7 9 2

11 DHKE computation

Suppose Alice and Bob want to use the Diffie-Hellman Key Exchange (DHKE) to agree upon a common key. Consider the following parameters:

- the group used is $\mathbb{Z}_{23} = \{0, 1, 2, \ldots, 22\}$.
- the generator used is $g = 5$.

Suppose furthermore, that Alice chooses the secret exponent $a = 3$ and Bob choose the secret exponent $b = 5$.

Perform the actions that Alice and Bob need to take in order to agree upon the common key, and compute the value of that key.

Fill in your answer here

Alice makes: g^a (mod Z_23) = 5^3 (mod 23) = 10
Then bob makes g^b (mod Z_23) = 5^5 (mod 23) = 20
Then they exchange this information and add their exponent to the mix
So that the private key becomes 10^5 (mod 23) = 20^3 (mod 23) = 19

Ord: 50

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

0 9 4 7 6 9 6

12 DHKE (other)

The Diffie-Hellman Key Exchange (DHKE) is not a cipher since it does not actually allow one to encrypt and decrypt messages. Which asymmetric cipher is based on the DHKE?

Using groups of the form $\mathbb{Z}_p$ requires the prime p to be very large in order for the DHKE to be secure since index calculus can be used to efficiently solve the discrete logarithm problem. What other algebraic group is used in the DHKE for which index calculus does not work (and which therefore allows the keys and modulus to be of significantly smaller size)?

Fill in your answer here

Elgamal is a asymmetric cipher based on DHKE.

The eliptical curve

Ord: 11

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

8 8 0 9 2 3 9

13 Hash functions

Define the notion of a hash function.

Name the three properties that cryptographic hash functions should have, and explain the relations between them.

Give some examples of applications of hash functions in cryptography.

Fill in your answer here

A hash function is a function that take an input of any length and its output is of a fixed length

Chinese remainder theorem (just mention it) :))

Ord: 28

Knytte håndtegninger til denne oppgaven?
Bruk følgende kode:

2 4 7 0 2 5 5