Special instructions for home exam in

EDIN01 CRYPTOGRAPHY

Dept. of Electrical and Information Technology Lund University

10.00 on April 22, 2020, until latest 12.00 on April 23.

- Hand-out of exam: at 10.00 on April 22 the exam will be available on the course web page for download. Use your own white sheets for writing solutions. Alternatively, a copy of the exam and empty sheets of paper can be picked up in boxes outside EIT (third floor in E-building) from 10.00.
- Hand-in of exam: During 10.00-12.00 on April 23 you can hand in your exam solutions at the department (third floor in E-building). Alternatively, you can hand in by scanning your solutions and email them to the examiner on email address: thomas@eit.lth.se no later than 12.00! But you must then also send the original solutions and this first page with original signature by regular mail to the address below.[1] The exam will not be corrected until this is received.
- Exam contents: In the home exam there will be problems similar to a standard exam. The grading will require 25/35/45 points for grade 3/4/5, respectively, out of a total of 50. To get grade 5 you additionally need to be approved on an oral exam.
- Sign-up: You need to have signed up to take the exam. You are not allowed to take the exam if you are already previously approved.
- Help and assistance: You are allowed to use any written information you have access to and you are allowed to use computers and programming for computations. **You are not allowed to get assistance in any way from any other person to help you with your solutions.** This includes asking people to post information on forums, etc. It also includes assisting any other person doing the exam. To assure this, you have to formally sign such a statement.[2] **This first page with original signature must be handed in together with your solutions!**

Name:

Personal Identifier:

I solemnly declare that I have not used help from any other person in the process of preparing the exam solutions that I now hand in.

Signature:

Hand in this page with original signature!

[1] Address: Education Office, Dept. of EIT, Box 118, 22100 Lund, Sweden

[2] Overstepping the rules of help and assistance may lead suspension from the university.

Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

April 22, 2020

- For questions on the exam, email the examiner.
- Each solution should be written on a *separate sheet of paper*.
- You must *clearly* show the line of reasoning.
- If any data is lacking, make reasonable assumptions.

Good luck!

Problem 1

In an RSA cryptosystem the public encryption function is $C = M^e \bmod n$ and the secret decryption function is $M = C^d \bmod n$, where M is the plaintext and C is the ciphertext. Let the public parameters of the RSA-system be denoted (n, e), where $n = pq$.

a) Choose a prime p such that $10000 \leq p \leq 11000$. Show the computational steps of a probabilistic primality test that shows that it is indeed most likely a prime.

(2 points)

b) Then pick the prime $q = 127$ and form the RSA public keys $(n = pq, e)$. Find the smallest possible choice for e with the condition $e \geq 20$ and give the secret parameters d and $\phi(n)$ in the RSA cryptosystem.

(3 points)

c) Show the steps of calculating the ciphertext $C = M^e \bmod n$ when encrypting the plaintext $M = 1357$ in your constructed RSA system. Use square-and-multiply or some similar efficient method.

(2 points)

d) In a broadcast scenario, Alice is sending the same message M to three different recipients with different public keys all with $e = 3$, say $(n_1, 3), (n_2, 3), (n_3, 3)$, where n_1, n_2, n_3 is of similar size. The ciphertexts are then given as $C_1 = M^3 \bmod n_1$, $C_2 = M^3 \bmod n_2$ and $C_3 = M^3 \bmod n_3$. Show how Eve can find the message (in an efficient way) after observing C_1, C_2, C_3.

(3 points)

Problem 2

b) Find the shortest linear feedback shift register that generates the sequence

$$s = [0, 1, 2, 2, 0, 2]^\infty$$

over $\mathbb{F}_3$.

(5 points)

a) Find the shortest linear feedback shift register that generates the sequence

$$s = (0, 1, \alpha, \alpha^2 + 1, \alpha + 1)$$

over $\mathbb{F}_{2^3}$ generated by $\pi(x) = x^3 + x + 1$ and $\pi(\alpha) = 0$.

(5 points)

Problem 3

a) A Shamir threshold scheme for $n = 5$ participants with threshold $k = 3$ using the public values $x_i = i$ is assumed. All values are assumed to be in $\mathbb{F}_{101}$. Participants 1, 2, and 3 hold the private shares $y_1 = 45$, $y_2 = 58$, and $y_3 = 61$. Help them to reconstruct the secret.

(5 points)

b) In an authentication system the source message S and the key E are given as,

$$S = (s_1, s_2), \quad E = (e_1, e_2),$$

where

$$s_1, s_2, e_1, e_2 \in \mathbb{F}_{101}.$$

The coded message M is a 3-tuple generated by

$$M = (s_1, s_2, t),$$

where

$$t = e_1 + s_1 e_2 + s_2 e_2^2.$$

Find a message that maximizes the chance of success in a substitution attack when the observed message is $M = (1, 1, 1)$.

Recall that P_S in general is calculated as

$$P_S = \max_{M, M', M' \neq M} P(M' \text{ valid} | M \text{ observed}).$$

(5 points)

Problem 4

Factor the RSA number $n = 44384521$ using the basic form of the Quadratic Sieve algorithm you learned in the first project. The square of the following numbers are B-smooth for some very small B,

$$1883840, 6521874, 13519124, 16006155.$$

Note that factoring n by trial division is not allowed. You need to document the solution steps in detail.

(10 points)

Problem 5

Consider the following problems on polynomials and fields.

a) Determine the full cycle set for the polynomial

$$C(D) = D^8 + D^7 + D^4 + D + 1$$

over $\mathbb{F}_2$.

(6 points)

b) How many elements of order 3 are there in $\mathbb{F}_{2^4}$?

(2 points)

c) Prove that $x^4 + x + 1$ is not irreducible ("primpolynom") over $\mathbb{F}_{2^4}$.

(2 points)

Some useful formulas in cryptology.

2013-12-07

Ch. 1: CRT: $x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_k \pmod{n_k}$, $\gcd(n_i, n_j) = 1, i \neq j$.

$$x = \sum_{i=1}^{k} a_i N_i M_i \bmod n,$$

where $N_i = n/n_i$ and $M_i = N_i^{-1} \bmod n_i$.

Ch. 2:

$$\begin{aligned} \text{M.R.} &= \sum_{i=A}^{Z} (p_i - \frac{1}{26})^2 = \sum_{i=A}^{Z} p_i^2 - 0.038 \\ \text{I.C.} &= \frac{\sum_{i=A}^{Z} f_i(f_i - 1)}{N(N-1)} \end{aligned}$$

Ch. 3:

$$\begin{aligned} I(X;Y) &= H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) \geq 0 \\ H(XY) &= H(X) + H(Y \mid X) = H(Y) + H(X \mid Y) \\ H(X) &= -\sum_i f_X(x_i) \log_2 f_X(x_i) \\ h(p) &= -p \log_2 p - (1-p) \log_2 (1-p) \end{aligned}$$

$$\begin{aligned} \text{Redundancy:} \quad D &= H_0 - H(M) \\ H(K \mid \mathbf{C}) &\geq H(K) - ND \\ N_0 &= H(K)/D \end{aligned}$$

Ch. 4:

$$\begin{aligned} S(D) &= \frac{P(D)}{C(D)} \\ 1(1) &\oplus 1(q^L - 1) \\ 1(1) &\oplus \frac{q^L - 1}{T}(T) \\ 1(1) &\oplus \frac{q^{L_1} - 1}{T_1}(T_1) \quad \oplus \cdots \oplus \quad \frac{q^{(n-1)L_1}(q^{L_1} - 1)}{T_n}(T_n); \\ & \quad T_j = p^i T_1, \; p^{i-1} < j \leq p^i \\ S_1 &\otimes S_2 \quad \otimes \cdots \otimes \quad S_m \\ & n_1(T_1) \otimes n_2(T_2) = (n_1 n_2 \gcd(T_1, T_2))(\operatorname{lcm}(T_1, T_2)) \end{aligned}$$

$$\begin{aligned} & \forall\, m_1, m_2, \ldots, m_r \in \mathbb{Z}^+ \,; \gcd(m_i, m_j) = 1, \; i \neq j \\ & \forall\, a, u_1, u_2, \ldots, u_r \in \mathbb{Z} \\ & \exists! u \in \mathbb{Z}^+ \; (a \leq u < a + m) \; \wedge \; (u_j = u \pmod{m_j}, \; 1 \leq j \leq r) \\ & \text{where} \quad m = m_1 m_2 \cdots m_r \end{aligned}$$

Ch. 6:

$$\begin{aligned} & n, m \in \mathbb{Z}^+ \\ & \phi(m) = |\{i \in \{1, 2, \ldots, m-1\} \mid \gcd(i, m) = 1\}| \\ & \forall n; \; \gcd(n, m) = 1 \; (n^{\phi(m)} = 1 \pmod{m}) \end{aligned}$$

Ch. 7:

$$\begin{aligned} P_D &= \max(P_I, P_S) \\ P_I &= \max_{\mathbf{m}} P(\mathbf{m} \text{ valid}) \\ P_S &= \max_{\mathbf{m},\mathbf{m}':\mathbf{m}\neq\mathbf{m}'} P(\mathbf{m}' \text{ valid}|\mathbf{m} \text{ valid}) \end{aligned}$$

Simmons bounds: $P_I \geq 2^{-I(\mathbf{M};E)}$
$P_S \geq 2^{-H(E|\mathbf{M})}$

Ch. 8:

$$a(x) = \sum_{i=1}^{k} y_i \prod_{1\leq j\leq k, j\neq i} \frac{x - x_j}{x_i - x_j}$$

The frequency of various letters in English text is given below. Out of 1000 letters the expected number of occurences for each letter is:

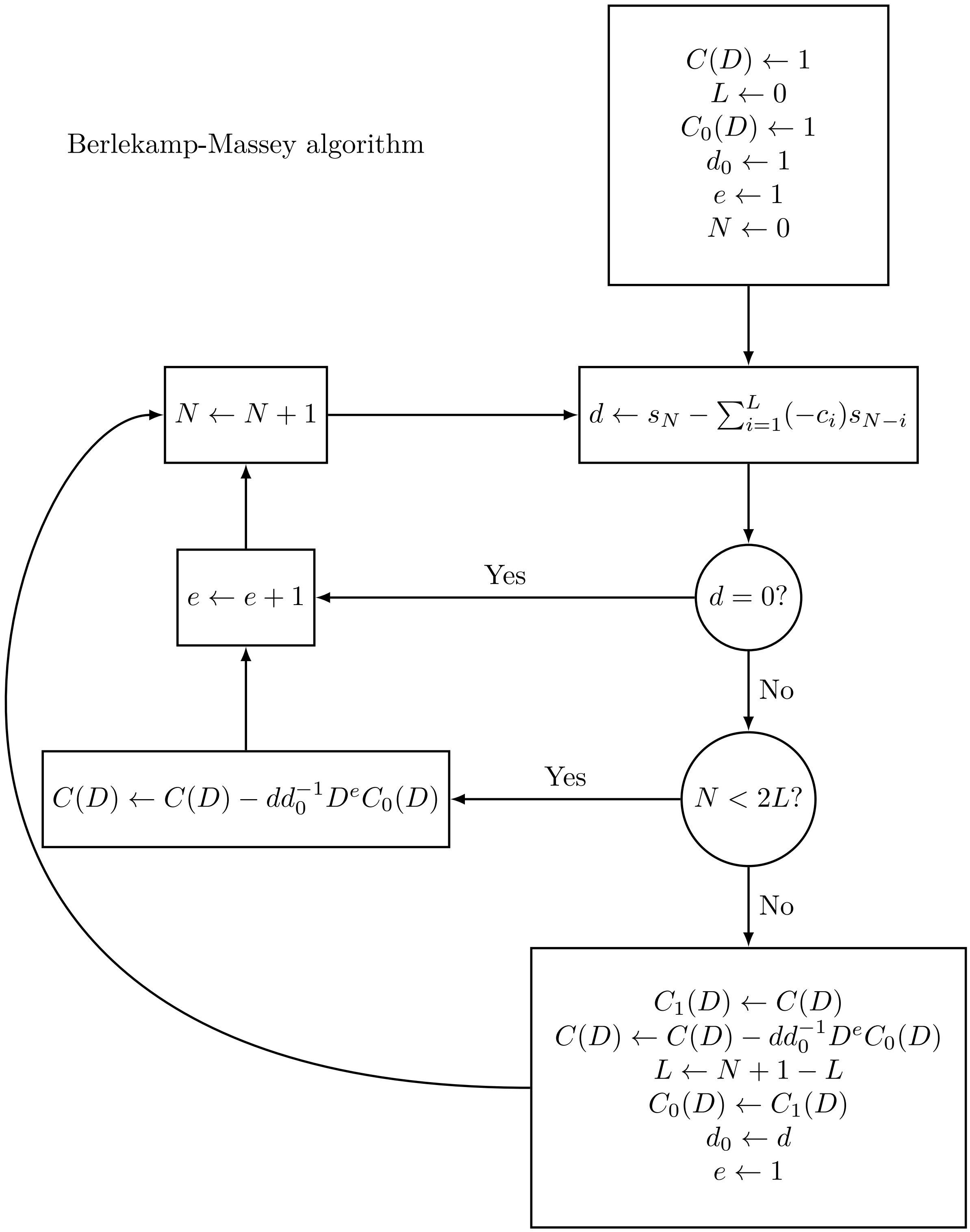
A	73	J	2	S	63
B	9	K	3	T	93
C	30	L	35	U	27
D	44	M	25	V	13
E	130	N	78	W	16
F	28	O	74	X	5
G	16	P	27	Y	19
H	35	Q	3	Z	1
I	74	R	77		

In a text of 80000 letters the most common bigrams and trigrams appear on average as given below:

TH	2161	ED	890	OF	731
HE	2053	TE	872	IT	704
IN	1550	TI	865	AL	681
ER	1436	OR	861	AS	648
RE	1280	ST	823	HA	646
ON	1232	AR	764	NG	630
AN	1216	ND	761	CO	606
EN	1029	TO	756	SE	595
AT	1019	NT	743	ME	573
ES	917	IS	741	DE	572

THE	1717	TER	232
AND	483	RES	219
TIO	384	ERE	212
ATI	287	CON	206
FOR	284	TED	187
THA	255	COM	185

Berlekamp-Massey algorithm



s_N	d	$C_1(D)$	$C(D)$	L	LFSR	$C_0(D)$	d_0	e	N
$-$	$-$	$-$	1	0	$\leftarrow$	1	1	1	0