Final exam in

CRYPTOGRAPHY

Dept. of Electrical and
Information Technology
Lund University

January 14, 2019, 14–19

- You are allowed to use a calculator.
- 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) One of the integers in $\{1041, 1043, 1047, 1049\}$ is a prime. Use a probabilistic primality test to determine which one. Call it p.

(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 $M = 2345$ in your constructed RSA system. Use square-and-multiply or some similar efficient method.

(2 points)

d) Give the arguments that show that decryption of a ciphertext C always returns the original message M (that created the ciphertext). (3 points)

Problem 2

Consider the following statements about the two polynomials $P_1(x) = x^5 + x + 1$ and the primitive polynomial $P_2(x) = x^4 + x + 1$.

a) The polynomial $P_1(x)$ is irreducible ("primpolynom") over $\mathbb{F}_2$.

b) The polynomial $P_1(x)$ is primitive over $\mathbb{F}_2$.

c) The cycle set for an LFSR with connection polynomial $C(D) = P_2(D)^2$ in $\mathbb{F}_2$ contains cycles of length 30.

d) Use $P_2(x)$ to construct $\mathbb{F}_{2^4}$ through $P_2(\alpha) = 0$. The element α^{10} has order 15.

e) The equation $x^2 + 1 = 0$ over $\mathbb{F}_{2^4}$ has a solution.

Choose for each of the five statements given above one of the following alternatives:

i) Correct — I am uncertain
ii) Wrong — I am uncertain
iii) Correct — I am certain
iv) Wrong — I am certain.

Correct answer according to i) or ii) gives 1 point.
Correct answer according to iii) or iv) gives 2 points.
Erroneous answer according to i) or ii) gives 0 points.
Erroneous answer according to iii) or iv) gives -2 points.

(Only answers are required!)

(10 points)

Problem 3

We wish to encrypt a source with alphabet $\mathbb{Z}_2^l$ generating independent symbols with $P(M = m) = 1/2^{l-1}$ for $m \in \mathcal{M}$ and $P(M = m) = 0$ for $m \notin \mathcal{M}$. Here $\mathcal{M}$ is the subset of $\mathbb{Z}_2^l$ where vectors start with a 0. We consider $l = 128$.

We use AES-128. The key $\mathbf{K}$ is then of size 128 bits. A sequence of message symbols $\mathbf{M} = (M_0, M_1, \ldots, M_{n-1})$ is encrypted to a sequence of ciphertext symbols $\mathbf{C} = (C_0, C_1, \ldots, C_{n-1})$ by ECB mode as

$$C_i = \text{AES}(M_i), \quad 0 \leq i \leq n - 1.$$

a) Compute the unicity distance N_0 according to the formula. (5 points)

b) The unicity distance predicts the number of symbols we need to observe before we can uniqly determine the key used. Explain the conditions for Shannon's model of secrecy and why the observation of more than N_0 ciphertext blocks does not mean that one can break the cipher. (2 point)

c) Suggest a modification to the above scheme in order to achieve $N_0 = \infty$. (3 points)

Problem 4

a) Five friends are sharing a key K through a secret sharing scheme. Three persons P_1, P_2, P_3 have private shares in a Shamir threshold scheme for 3 participants with threshold $k = 2$ using the public values $x_i = i$. Furthermore, P_4 has a share y_4 and P_5 has a share y_5, where these shares have been chosen in such a way that $K = y_4 + y_5$. All values are assumed to be in $\mathbb{F}_{19}$.

- Write up the access structure for the construction.
- Explain why the construction gives an ideal secret sharing scheme.
- Assume that P_2 holds the private share $y_2 = 3$, and P_3 holds the private share $y_3 = 10$. Reconstruct K.

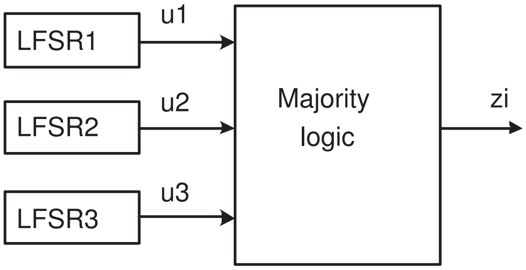
(5 points)

b) In an authentication system, Alice would like to send a source message $s \in \mathbb{Z}_q$ to Bob in an authenticated channel message M.

They are using an authentication code, where the key (encoding rule) E is given as $E = (e_1, e_2)$, where $e_1, e_2 \in \mathbb{Z}_q$. The transmitted message is $M = (s, t)$, where $t = e_1 + se_2$. Prove that $P_I = P_S = 1/q$ if q is a prime, and show that this is not true if q is a composite.

(5 points)

Problem 5



Alice encrypts her plaintext using a simple stream cipher, built as in the figure above. The keystream symbol is determined from the output of the LFSRs in the following way. If two or three output symbols from the LFSRs are one, the keystream symbol will be one, otherwise it will be zero. The secret key K is the initial state of the three LFSRs. Hence, we can write the key as a 3-tuple, $K = (K_1, K_2, K_3)$, where K_i is the initial state of the i^{th} LFSR. The connection polynomials for the different LFSRs are $C_1(D) = 1 + D + D^4$, $C_2(D) = 1 + D + D^3$ and $C_3(D) = 1 + D + D^2$.

Determine the key (initial states) when it is known that the keystream output is

$$\mathbf{z} = 0011\ 1110\ 1011\ 0110\ 1111\ 1001\ 0110\ 0101\ 1011.$$

(10 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:

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

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

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:

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

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

Ch. 8:

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

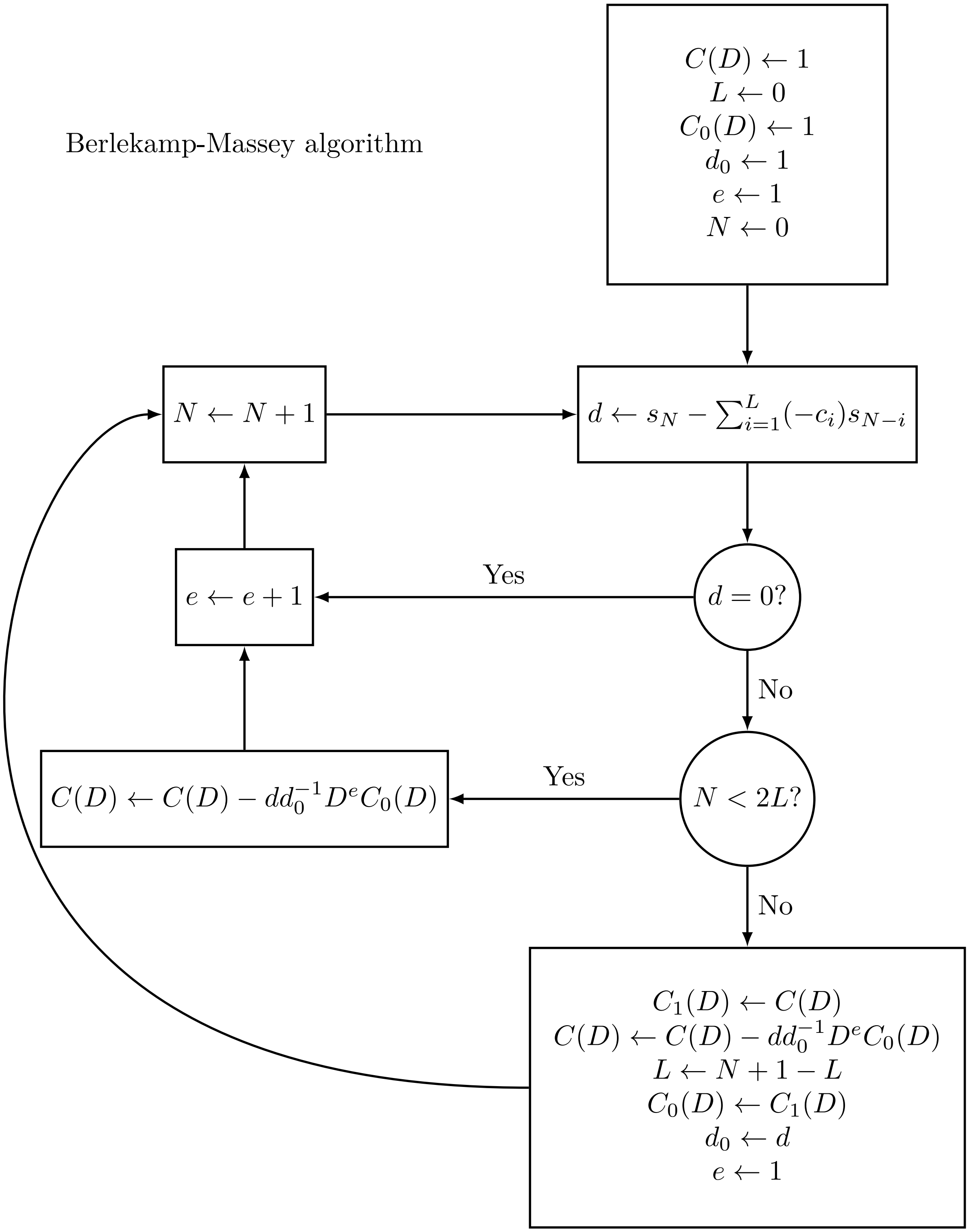
The frequency of various letters in English text is given below. Out of 1000 letters the expected number of occurences for each letter is:

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	THE	1717	TER	232
HE	2053	TE	872	IT	704	AND	483	RES	219
IN	1550	TI	865	AL	681	TIO	384	ERE	212
ER	1436	OR	861	AS	648	ATI	287	CON	206
RE	1280	ST	823	HA	646	FOR	284	TED	187
ON	1232	AR	764	NG	630	THA	255	COM	185
AN	1216	ND	761	CO	606				
EN	1029	TO	756	SE	595				
AT	1019	NT	743	ME	573				
ES	917	IS	741	DE	572				

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