40 5.

CHALMERS
EXAMINATION / TENTAMEN

Course code/kurskod	Course name/kursnamn		*
TDA352	Cryptography		X
Anonymous code Anonym kod	Examination date Tentamensdatum	Number of pages Antal blad	Grade Betyg
TDA352-6	2018-01-12	6	5

* I confirm that I've no mobile or other similar electronic equipment available during the examination.
Jag intygar att jag inte har mobiltelefon eller annan liknande elektronisk utrustning tillgänglig under examinationen.

Solved task Behandlade uppgifter No/nr		Points per task Poäng på uppgiften	Observe: Areas with bold contour are to completed by the teacher. Anmärkning: Rutor inom bred kontur ifylles av lärare.
1	X	6	
2	X	8	
3	X	15	
4	X	11	
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
Bonus credits/ poäng			
Total examination points Summa poäng på tentamen		40	

Family name+First name (Blockletters) Efternamn+Förnamn+Initialer(textas)	Signature Namnteckning	Year of Admission Antagningsår	Programme acronym Program	Identification no nummer
THORSELL ERIK E.T				

Date of Birth Year Month Day
Personnummer
år mån dag

Symmetric Ciphers

a) Using a key of length $|k|$ we can encrypt arbitrarily long messages by extending the key as below. So $|m|$ must not be known

$m = m_0\ m_1\ m_2\ m_3\ m_4$

$k = k_0\ k_1\ k_2$

$C = m_0 \oplus k_0 \quad m_1 \oplus k_1 \quad m_2 \oplus k_2 \quad m_3 \oplus k_0 \quad m_4 \oplus k_1$

Decryption is done analogously: $m = c_0 \oplus k_0$ ..

0

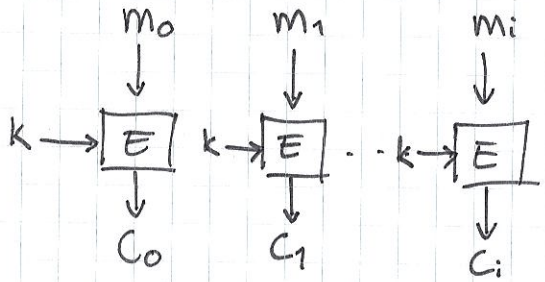
b) It is possible to acquire a PRG from a PRF, by feeding the PRF $F(k, m) \rightarrow C$ with different keys: $k_0, k_1, k_2, \ldots$ and a fixed m.

The outputs will be indistinguishable from output drawn from the uniform distribution.

2 Kinda Yes

c)

ECB



$c_i = E(k, m_i)$
$m_i = D(k, c_i)$

m_i are blocks of equal length
k is the key

1

d)

Semantic Security

A wins if he can guess if $c_b = E(k, m_0)$ or $c_b = E(k, m_1)$ with ~~non~~ unneglegible certainty.

If A sends two messages with two blocks each he can win the game.

Let $m_0 = m||m$ and $m_1 = m||\hat{m}$, m and $\hat{m}$ are 1 block big. Due to the blockwise encryption of ECB, A can learn how m is encrypted and therefore tell ~~which~~ if $c_b = C||C$ or $c_b = C||\hat{C}$. If the encrypted block's does not match, C encrypted m_1 and vice versa.

3 Missing $P(Adv) = 1$

5

Public Key Encryption

a) ElGamal

1: $\text{keygen}(\lambda) \rightarrow (S_k, P_k)$

Let q be a λ-bit integer and let g be a generator for the group G. $|G| = q$

Let x be a random number from $\{1, \ldots, q-1\}$

Let $h = g^x$

$S_k = \langle x \rangle$

$P_k = \langle G, g, q, h \rangle$

2: $\text{Encryption}(P_k, m) \rightarrow c$

$E(P_k, m) = c$ where $c = (c_1, c_2)$

$c_1 = g^r$ where $r \leftarrow_R \{1, \ldots, q-1\}$

$c_2 = h^r \cdot m$

3. $\text{Decryption}(S_k, c) \rightarrow m$

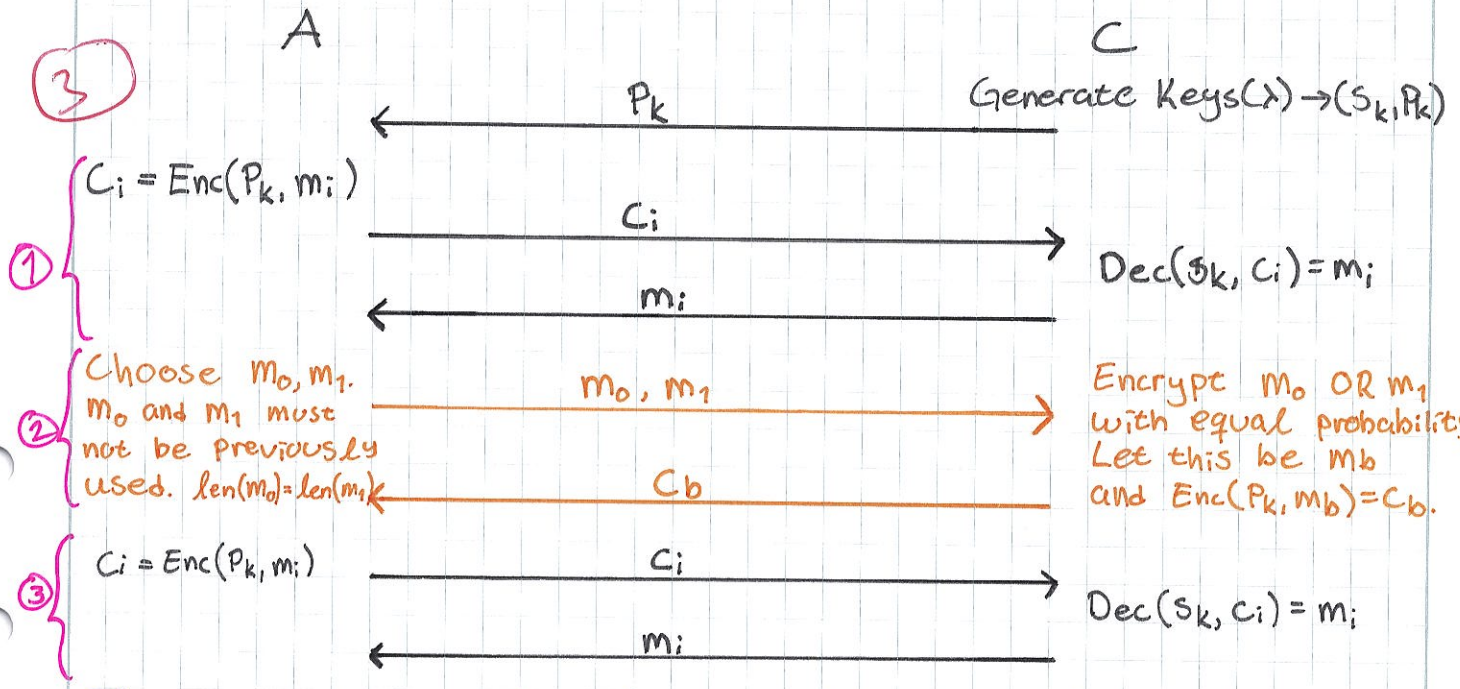
$(c_1, c_2) = c$

$m = c_1^{-x} \cdot c_2$

b) The discrete log problem states that is computationally infeasible to acquire x from a^x given a.

5

c) IND-CCA



The adversary wins if (s)he is able to tell if C_b is the enc of m_0 or m_1 with unneglegible certainty.

1: Query Phase 1, the adversary may send polynomially many queries.

2: Challenge Phase

3: Query Phase 2, see 1.

d) Due to the homomorphic properties of ElGamal encryption, an adversary can win IND-CCA.

If A sends $m_1 = m$ in the first query phase and $m_1 = 2 \cdot m$ in the challange phase (along with $m_2 = \hat{m}$), he can tell if C_b is twice the C_i corresponding to the aforementioned m_i.

If so: $C_b = Enc(P_k, m_1)$ else $C_b = Enc(P_k, m_2)$.

5

Data Integrity

a) RSA

1. Keygen(λ) $\rightarrow$ (d, e)

Let p, q be λ-bit primes and let $N = p \cdot q$

Let $e \xleftarrow{R} \{1, \dots, \Phi(N)\}$ s.t. $\gcd(e, \Phi(N)) = 1$

Let $d = e^{-1} \bmod \Phi(N)$ Let $S_k = (N, d)$, $P_k = (N, e)$

2. Encryption(e, m) $\rightarrow$ c

$C = m^e \bmod N$

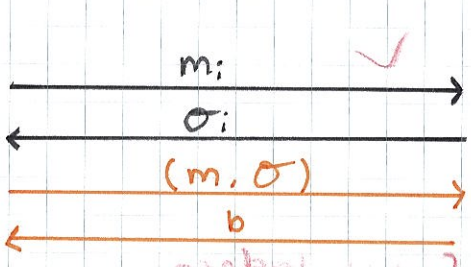
3. Decryption(d, c) $\rightarrow$ m

$m = c^d \bmod N$

b) $E(e, m_1) \cdot E(e, m_2) = m_1^e \cdot m_2^e = (m_1 \cdot m_2)^e = E(e, m_1 \cdot m_2)$

c) Existential forgery states that it is possible for an adversary to create a (m, σ) tuple which gets approved, even though the adversary did not have the key required to sign the message.

EX-FORGE GAME



d) If A has C sign two msg m_1, m_2 he receives σ_1, σ_2. Due to the homomorphic properties of RSA $m = m_1 \cdot m_2$ will have signature $\sigma = \sigma_1 \cdot \sigma_2$. Hence A can send m and σ to C and win the game.

e) This can be avoides by introducing hashing, since that elliminates the issues with homomorphism. $h(m_1) \cdot h(m_2) \neq h(m_1 \cdot m_2)$ Sign the hash of the message!

f) 1. Non-repudiation, due to the use of a private key for signing.

2. Assymetry! Need not a shared, secret, key but can verify with P_k.

3.

CHALMERS	Anonymous code / Anonym kod	Points for question (to be filled in by teacher) / Poäng på uppgiften (ifylles av lärare)	Consecutive page no. Löpande sid nr 5
	TDA352-6		Question no. Uppgift nr 4

Cryptographic Protocols

a)

i. The correctnes property states that a true prover will be identified by the verifier correctly. This is done by performing the computation below.

$$R = g^s \cdot X^{-c} = g^{r+cx} \cdot g^{-xc} = g^r = R$$

2

ii. Due to the characteristics of the protocol, it is not possible for the verifier to transfer knowledge about a prover. Peggy most prove herself to all verifiers she wants to gain trust from.

Since Victor knows nothing of x, only that Peggy seems to posses it, there is no use in him telling others.

iii. If Peggy uses the same $R = g^r$ in two different executions of the protocol, it is possible for Victor to gain knowledge about x.

0.5

By chosing c s.t. it counteracts some part of R, A can gain knowledge of x. I've forgotten how though...

5

b)

3 parties; $P_1, P_2, P_3 \Rightarrow n=3$, we know $t=1$

$a=3$
$b=5$
$c=2$

i. Each Party determines a polynomial of degree 1.

$f_1(x) = x+3$
$f_2(x) = 2x+5$
$f_3(x) = 3x+2$

They know compute three shares each, to be distributed among the parties.

$a_1 = f_1(1) = 1+3 = 4$ $\quad b_1 = f_2(1) = 2+5 = 7$ $\quad c_1 = f_3(1) = 3+2 = 5$
$a_2 = f_1(2) = 2+3 = 5$ $\quad b_2 = f_2(2) = 4+5 = 9$ $\quad c_2 = f_3(2) = 6+2 = 8$
$a_3 = f_1(3) = 3+3 = 6$ $\quad b_3 = f_2(3) = 6+5 = 11$ $\quad c_3 = f_3(3) = 9+2 = 11$

$\sigma_1 = a_1 + b_1 + c_1 = 4+7+5 = 16$
$\sigma_2 = a_2 + b_2 + c_2 = 5+9+8 = 22$
$\sigma_3 = a_3 + b_3 + c_3 = 6+11+11 = 28$

$\sigma = a+b+c = 3+5+2 = 10$

	P_1	P_2	P_3
$a=3$	4	5	6
$b=5$	7	9	11
$c=2$	5	8	11
$\sigma=10$	16	22	28

3

ii. We use Lagrange interpolation*

$S = \delta_1\sigma_1 + \delta_2\sigma_2 + \delta_3\sigma_3 = 3\cdot 16 - 3\cdot 22 + 1\cdot 28 = 10$

3

* I think it's called that.

$\delta_i = \prod_{\substack{j=1 \\ j\neq i}}^{n} \left(\frac{j}{j-i}\right)$ $\qquad \delta_1, \delta_2, \delta_3 = ?$

iii. Since $t=1$ we can allow for one corrupted party.

$S = 2\cdot 16 - 1\cdot 22 = 10$

2.5

Note that δ_i now spans $\{1,2\}$ not $\{1,2,3\}$ as in ii.