Winter 2010, A

Question 1 (34 points)
An Independent Set (IS) in a graph $G=(V,E)$ is a set of vertices $U \subseteq V$ such that $(u,v) \notin E$, for every two vertices $u,v \in U$.

Given a graph $G=(V,E)$ and $k \in \mathbb{Z}$, the decision problem: “Is there an independent set of size at least $k$ in $G$” is NP-complete.

Describe a ZK protocol for the independent set problem (i.e., given a graph $G$ and $k \in \mathbb{Z}$, allows to prove that $G$ has an independent set of size at least $k$).

Prove that your protocol is indeed an interactive proof, and show that it is ZK.

Is your protocol perfect ZK, or computational ZK?

Note: When analyzing probabilities, you don’t have to calculate the accurate numbers, you can just give a formula from which the probability can be computed, and explain why it fits the requirements.

Question 2 (22 points)
Let $p$ be a large prime. In class we saw that given the factorization of $p-1$ to prime factors, we can efficiently find a generator of $\mathbb{Z}_p^*$, by choosing random numbers and checking whether they are indeed a generator of the group.

A. Express the probability that a random element in $\mathbb{Z}_p^*$ is a generator, and explain your answer briefly.

B. Let $n = p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}$ be a number such that $p_1 < p_2 < \ldots < p_k$ are the prime factors of $n$. Prove that for every $1 \leq i \leq k$ it holds that $1 - \frac{1}{p_i} \geq 1 - \frac{1}{i+1}$.

C. Prove that the method we saw in class for finding generators of $\mathbb{Z}_p^*$ (described above) is efficient.
Question 3 (22 points)
The decisions of the government on the planet Krypton have to be made unanimously. If at least one of the cabinet members objects to the motion, the motion is rejected.
In order to validate a motion $m$, $x=H(m)$ has to be signed using the RSA signature scheme, where $h$ is a secure hash function. The public key of the government is known to everyone in the galaxy.

In order to prevent the Cabinet Secretary from signing motions which were not unanimously approved by the cabinet, the secret key was shared between the cabinet members, such that it is only possible to generate a legitimate signature if all of them cooperate.
The scheme should allow usage of the shared secret key for signing more than one motion.

Suggest a scheme for sharing the secret key between the cabinet members. Explain how the key is shared, how a signature is generated (what computations are made by the cabinet members? What computations are made by the Cabinet Secretary?). Prove the correctness of your scheme, and discuss its security.
**Question 4 (22 points).**

In the Merkle-Damgard scheme (slides 181-182) a message of arbitrary length is hashed by dividing it to blocks of fixed length: \(M_1, M_2, \ldots, M_l\). The compression function \(h_i = C(h_{i-1}, M_i)\) compresses the previous chaining value \(h_{i-1}\) and the current message block \(M_i\), and generates a new chaining value \(h_i\).

The value \(h_0 = IV\) is fixed and known to everyone, and the resulting hash value is the last chaining value \(h_l\), as seen in the figure.

In SHA-1 the compression function follows the Davis-Meyer (DM) construction:
\[
h_i = C(h_{i-1}, M_i) = E_M (h_{i-1}) + h_{i-1}, \quad \text{where } E \text{ behaves like a block cipher.}
\]
The IV, the chaining values \((h_i)\), and the hash value are all 160 bit long. The message blocks \(M_i\) are 512 bit long.

A. Explain why the Davis-Meyer structure is necessary (adding \(h_{i-1}\) at the end of the compression function). I.e., show a possible attack which is possible if the compression function is of the form: \(h_i = C(h_{i-1}, M_i) = E_M (h_{i-1})\), but is not possible with the DM addition.

B. Tamar claimed that it was not necessary to perform the DM addition in every single block, and that it was enough to perform it once on all the blocks together. I.e., hashing will be done by:
\[
h_i = \begin{cases} 
E_M (h_{i-1}) & 1 \leq i \leq l - 1 \\
E_M (h_{i-1}) + h_0 & i = l
\end{cases}
\]
Does the attack from A still work? Is the new method vulnerable to other attacks on hash functions (which DM protects against)?

C. Ronen claimed that if we are going to perform the DM protection only once, we should do it on the last block. I.e., hashing will be done by:
\[
h_i = \begin{cases} 
E_M (h_{i-1}) & 1 \leq i \leq l - 1 \\
E_M (h_{i-1}) + h_{i-1} & i = l
\end{cases}
\]
Does the attack from A still work? Is the new method vulnerable to other attacks on hash functions (which DM protects against)?

D. Yafit claimed that in order to increase the mixing between the blocks of the message we should perform the hashing in the following way:
\[
h_i = \begin{cases} 
E_M (h_{i-1}) + h_{i-1} & \text{if } i \text{ is odd} \\
E_M (h_{i-1}) + h_{i-2} & \text{if } i \text{ is even}
\end{cases}
\]
Does the attack from A still work? Is the new method vulnerable to other attacks on hash functions (which DM protects against)?

**Winter 2009, A**

**Question 1**

This question deals with the Goldwasser-Micali (GM) probabilistic encryption scheme, which was the first probabilistic scheme ever suggested.

In a probabilistic encryption scheme the value of the ciphertext depends on a random value which is chosen in the process of encryption (and, of course, on the value of the plaintext). Therefore, every time the same message is encrypted, we expect to get a different ciphertext.

A. Describe two advantages of a probabilistic encryption scheme (over a deterministic public-key encryption scheme).

Key Generation in the GM scheme:

1. Randomly choose \( p, q \) large primes.
2. Compute \( n = pq \)
3. Choose \( y \in \mathbb{Z}_n^* \), such that \( y \) is a QNR modulo \( n \), whose Jacobi symbol is 1.
4. The public key is \((y, n)\). The private key is \((p, q)\).

B. Show how we can efficiently (probabilistically) find \( y \) as required in step 3.

C. A student in the course “Prime Number Theory” claimed that by choosing \( p, q \) carefully, we can find such \( y \) deterministically. How will he choose \( p, q \)? What is the value of \( y \)?

The encryption algorithm encrypts a single bit. In order to encrypt longer messages, we encrypt each bit separately:

1. Choose \( x \in \mathbb{Z}_n^* \).
2. If \( m = 1 \) then \( c \leftarrow y \cdot x^2 \mod n \)
   
   Else \( c \leftarrow x^2 \mod n \)
3. The ciphertext is \( c \).

D. Explain how ciphertexts are decrypted in the GM system.

E. Show that breaking the GM encryption is at least as hard as deciding whether an element with Jacobi symbol 1 is a QR in \( \mathbb{Z}_n^* \).

Hint: show that the ciphertexts are uniformly distributed over all the numbers with Jacobi symbol 1 modulo \( n \).
F. What is the ratio between the size of the message space and the size of the ciphertext space in GM?
   Can there be a probabilistic encryption scheme where this ratio is 1? If you answer is yes – demonstrate. If your answer is no – explain why.

G. Prove that the GM scheme is random-self-reducible.
   Hint: show that given an algorithm which breaks GM on 1% of the inputs (and returns \( \bot \) for the other 99%), we can break GM on all inputs with probability better than 0.5.

**Question 2**

In the planet Krypton, elections to the House of Representatives are scheduled for next month. 64 parties are competing. The great magician Shikriyahu would like to convince the Kryptonites (inhabitants of Krypton) that he can predict the election results. For that purpose, Shikriyahu uses the hash function SHA-1 to hash a message of seven blocks \( M = M_0M_1\ldots M_6 \), where the first block contains the name of the party he believes will win the election, and the next six blocks \( M_1\ldots M_6 \) are chosen randomly.

Shikriyahu publishes the hash value of \( M \) as the commitment. Immediately after the real election results are published, Shikriyahu reveals the message \( M \).

Reminder: The block length of SHA-1 is 512 bits, the length of the hash value is 160 bits. Before encryption, the message is padded and the message length is concatenated to it.

A. Explain the importance of adding randomness to the hashed message.

B. Show how Shikriyahu can succeed in his prediction, no matter which party actually wins the election (by performing a pre-computation). What is the complexity of the required pre-computation?

**Question 3**

Was asked as part of the HW in the sixth home exercise.
Question 4

The cipher $\text{DES} \rightarrow 2$ is based on the cipher DES, with a minor change in the F function:

After the expansion function $E$, we add a cyclic rotation of two bits to the right (see figure).

Discuss the security of the new cipher against differential cryptanalysis.

Describe the best characteristic you can find, and explain how it is possible to use it to attack the cipher.

What is the probability of the characteristic? What is the complexity of the attack?

For your convenience, differential distribution tables are attached to the exam form.