NOM : **Prénom :** **Place :**

MASTER SCCI 7 November 2011

Security models: provable security

Time: 45'.

Very important:

- **Exercises are independent.**
- **Answer directly on the form; put you NAME and First name on the first page.**
- **The mark will take into account quality of presentation.**

Entropy and perfect secrecy

1. Let A, B, C be three random variables that verify: $H((A,B)|C) = H(A) + H(B|C)$.
What can be said about A, B and C – check the correct answer(s) – :
☐ Nothing (equality always verified) ☐ A, B are independent ☐ A, C are independent
☐ B, C are independent

2. A TripleDES key K contains 3 DES keys each with 8 bytes, so 24 bytes for $K = [B_1, \ldots, B_{24}]$. Each byte B_i is built as follows: a random integer is uniformly chosen in $\{0, \ldots, 127\}$ which defines the 7 first bits of B_i; the last bit of B_i is then the "xor" of its 7 first bits.
What is the entropy of the byte B_i? **Answer:**
What is the entropy of K? **Answer:**

3. Let n be an integer and $G = \mathbb{Z}/n\mathbb{Z}$. Consider the cipher with secret key $k \in G$ defined by: $\forall x \in G : C_k(x) = x + k \mod n$.

1. How to encrypt with unconditional security a message of size $m \gg log_2 n$ bits using this cipher ?
2. What n is required to ensure unconditional security ? ☐ any $n > 1$ ☐ any large n (eg 2048 bits)
   ☐ any large prime n (eg 2048 bits) ☐ any $n = pq$ with p and q 1024-bit primes

Complexity

4. On what problem(s) relies the security of the following protocols: (0.5 by correct answer, -0.5 by erroneous answer, bonus +0.5 for the three correct)

- RSA: ☐ SUBSET-SUM (mod m) ☐ LOG_G ☐ PLOG_G
  ☐ INTEGER-HAS-BIG-FACTOR ☐ INTEGER-FACTORIZATION ☐ QUADRATIC-RESIDUE
- Merkle-Hellman: ☐ SUBSET-SUM (mod m) ☐ LOG_G ☐ PLOG_G
  ☐ INTEGER-HAS-BIG-FACTOR ☐ INTEGER-FACTORIZATION ☐ QUADRATIC-RESIDUE
- El Gamal: ☐ SUBSET-SUM (mod m) ☐ LOG_G ☐ PLOG_G
  ☐ INTEGER-HAS-BIG-FACTOR ☐ INTEGER-FACTORIZATION ☐ QUADRATIC-RESIDUE

5. Briefly (but precisely) justify:

1. $P \subset NP$:
2. $(P \neq co-NP) \Longleftrightarrow (P \neq NP)$:

6. Let Q be a problem that takes in input: $\begin{cases} k : \text{an integer} \\ M \in \{0,1\}^{n \times m} \text{ a matrix } n \times m \text{ with entries in } \mathbb{F}_2. \end{cases}$

1. What is the input size (in order) ?
2. What is the cost (in O notation) of a polynomial time algorithm ?

Arithemtic and cryptography

7. Let $p \geq 3$ be a prime integer and $q = (p-1)/2$; let β be a primitive element mod p.
Prove that $\beta^q = -1 \bmod p$.

Exercice hash function

Let h be a compression function $\{0,1\}^{k+r} \longrightarrow \{0,1\}^r$.
Let H be the hash function built from h by Merkle-Damgard iterative scheme.

8 (4 points).

1. Provide a brief drawing of Merkle-Damgard scheme.
2. What is the condition on h that ensures H to be resistant to collisions?
   Answer:
   How would you prove it? Just give the principle of the proof.
   Answer:
3. Assume that a collision is known on H. How to generate many other collisions.

9. For a hash function with block size $k = 1000$ bits and message digest $r = 400$ bits, we consider the following padding of a message of m bits. Let $l = \lceil \log_2 m \rceil$ and $m = 2^l + \sum_0^{l-1} m_i 2^i$. Let $a = m \mod 1000 - l$ (note that a may be 0): the message is completed (as suffix) by a symbol "0" followed by 1, $m^{l-1}, \ldots, m_0$, in this order.
Is this padding secure ? (Justify briefly but precisely)

Complexity

10. Let Q be a problem that takes in input: $\begin{cases} k : \text{an integer} \\ B \in \{0,1\}^n \text{ an array of } n \text{ bits.} \end{cases}$

1. What is the input size? [mark by X the correct answer]

   $\square \log k + \log n \quad \square k + \log n \quad \square n + \log k \quad \square n + k$

2. Among the following complexities, which one(s) are polynomial in the input size of Q ?

   $\square O(\log^5 k.\log^2 n) \quad \square O(k^5.\log^2 n) \quad \square O(n^5.\log^2 k) \quad \square O(n^5.k^2) \quad \square O(5^n.k^2) \quad \square O(n^5.2^k)$