Cryptography, WPPT, M.Kutyłowski, preparation problems for 27.11.2013

Niniejsze zadania mają przygotować do kolokwium. Zalecamy rozwiązać je i przemyśleć. Pytania w dniu 27.11.2012 będą podobne w zakresie zarówno obszaru tematycznego jak i samej metodyki rozwiązania.

Szczegółowe instrukcje na egzamin:

- Można korzystać z dowolnych materiałów nieelektronicznych.
- Odpowiedzi na pytania na kartce z zadaniami. Ewentualne dodatkowe strony należy oddać podpisane.
- Odpowiedzi powinny koncentrować się na kluczowych zagadnieniach. Przytaczanie definicji nie jest punktowane (to nie jest test umiejętności przepisywania notatek). **Teksty nie na temat** wpływają **negatywnie** na ocenę.
- Można odpowiadać po polsku, angielsku. Poprawność językowa nie podlega ocenie, ważna jest jasność przekazu. **Tekst nieczytelny** pod względem graficznym **nie jest brany pod uwagę** (z wyjątkiem orzeczonego przypadku dysgrafii).
- Za każde zadanie można dostać 3 punkty.
- Wyniki będą dostępne na stronie WWW wykładu w prywatnej części z użyciem pseudonimów.

Problem 1. (a) Alice has sent an ElGamal ciphertext c to Bob. You wish only to know whether c is a ciphertext of m. Do you have any chance if you have only the public keys?

(b) Given an ElGamal ciphertext c. Is there any method that would indicate that c has been created with the public keys of Alice?

(c) A spy Kubuś 007 sends a secret message m to his boss. For this purpose he sends an ElGamal ciphertext to his email address from an Internet bar. He knows that the boss has access to the network and can copy the ciphertext. On the other hand, Kubuś 007 has to be careful and must not obtain any suspicious data. Check if this is possible. If yes, then show a concrete scenario. If not, then prove that this is impossible.

Problem 2. (a) You are given two security policy documents: Policy A states that the CBC encryption mode should be used with the initial vector IV equal to the serial number of the ciphertext. Policy B states that the user is free to apply any way of choosing IV. Which Policy is better? Or both are ok (or false)?

(b) Is it dangerous if two different users apply the same initial vector for the CBC encryption mode?

(c) Assume that the plaintext of one of the blocks in a CBC ciphertext has been revealed. Does it bring any threats for the security of the remaining blocks?

Problem 3. (a) Consider an authentication protocol: Alice chooses random a, computes $c_a = g^a$ and sends c_a to Bob. Bob computes $c_b = g^b$ and sends c_b to Alice. Alice computes $k = c_b^a$, her signature $s = \text{sign}(c_b)$ and ciphertext $\text{Enc}_k(s)$. She sends $\text{Enc}_k(s)$ to Bob, who computes $k = c_a^b$, decrypts and verifies signature s. Is this protocol a zero-knowledge protocol? Why? (attention: this is a tricky question)

(b) The following authentication protocol has been designed by Schnorr for a group of prime order and a generator g. Alice's secret key is a and her public key is $v = g^{-a}$. First Alice chooses r at random, computes $x = g^r$ and sends it to Bob. Bob responds with a random e. Alice computes $y = a \cdot e + r$. Bob checks whether $x = g^y \cdot v^e$.

Show that executing this protocol multiple times does not help the adversary to derive the secret of Alice.

Problem 4. (a) What happens if a hash function used for Schnorr signatures turns out to have a collision? Is it possible to derive the secret key?

(b) Assume that a company Kryptoprzewa?ka Sp.z.o.o. has modified the Schnorr signatures so that it computes $e = \text{Hash}(M \text{ xor } r)$ instead of $e = \text{Hash}(M, r)$. Is it as secure as the original version? Why?