CRYPTOGRAPHY and SECURITY,
preparatory problems for exam, January 2016

Name: ....

index number: ....

Problem 1 Write a TOE Summary corresponding to a remote password authentication based on the SRP protocol (some parts simplified):

initialization : Carol chooses a password p, a random salt s, and computes $x = \text{Hash}(s, p)$, $v = g^x$. The server stores (s, v) and index i to this entry.

remote authentication :

1. Carol chooses a at random and sends to the server: $A = g^a, i$
2. the server chooses b at random and replies with $B = 3v + g^b$
3. both parties compute $u = \text{Hash}(A, B)$
4. the server computes $K := \text{Hash}((A \cdot v^u)^b)$
5. Carol computes $K := \text{Hash}((B - 3v)^{a+ux})$
6. Carol and servers exchange tags that presumably show that both of them know K (details omitted)

Your duty is to find all advantages that SRP has, and formulate a corresponding Protection Profile. Now, you have to create the most synthetic part of PP – TOE Summary.

Problem 2 Assume that you are responsible for formulating and eIDAS extension that will explicitly refer to password authentication. Formulate the annex that specifies necessary conditions for secure password authentication. It should mimic the style of the existing formulations, e.g. the following one

> An advanced electronic seal shall meet the following requirements:
>
> (a) it is uniquely linked to the creator of the seal;
>
> (b)it is capable of identifying the creator of the seal;
>
> (c)it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
>
> (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

The answer in any official language of EU will be accepted.

Problem 3 During the lecture we have not discussed details of Pseudonymous Signatures from BSI technical recommendation on eIDAS Token. Look into the original report and find out all data concerning generation of the sector public key used for generating a pseudonymous signature. Write a report who and how can potentially break anonymity by linking signatures in different domains.

Problem 4 We have looked into Intel deterministic RNG as an example for the threats of hardware Trojans. Propose alternations to this PRNG that could improve the situation or enable to detect the problem.

Problem 5 Sometimes we are coerced to create a signature. Design a system for "dual-PIN" signing cards that enable you to sign transactions to your bank, enable your bank to detect that you have been coerced to do it, but at the same time the criminal coercing you may not detect that the signature contains a hidden warning to the bank.

Problem 6 As a defense against attacks on TLS/SSL with CBC encryption mode one can propose to encrypt blocks that consist of message bits (the first half of the block) and random bits (the second half of each block). How effective this method is against the attacks we have learnt.

Problem 7 To defend against cache attack Kubuś Puchatek proposed to store the lookup tables in a different way: the ith entry is stored at position $\pi(i)$. Does it work?

Problem 8 Read RFC2560 on OCSP. Now, you get an answer from an OCSP server that states that the certificate is valid. What the answer really means?