CRYPTOGRAPHY and SECURITY,
preparation for exam, Feb 3, 2017

Name: .....
index number: .....

Problem 1 Assume that you are responsible for formulating an eIDAS extension. We have to describe a trust service "confidential delivery" which can be implemented with good asymmetric encryption. Namely, instead of sending M in plaintext you send $\mathrm{Enc}_K(M)$, where K is the public key of the recipient. Formulate the annex that specifies general necessary conditions for such services. Of course, there are many ways to apply strong public key encryption so that the result is insecure, hence the task is not that trivial. Keep in mind that may be not only public key encryption may be used...

Your text should follow 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.
```

Problem 2 One of the crucial features of the attack against MD5 was that certain portion of the input to be hashed has been used more than once on specific positions during one application of the MD5 block compression function.

So let us modify MD5 so that each such portion of the input is used only once. Does such a modification solve the problem?

Problem 3 We have looked into a deterministic PRNG as an example for the threats of hardware Trojans. The presented scenario assumes that not all operations on the chip are predictable by the attacker - only some parts of the chip are corrupted and provide predictable results regardless of the seed. This complicates the seed recovery by the attacker.

Why not to corrupt most of the circuitry in order to reduce the effort of the attacker?

Problem 4 In the FIPS definition of hash based PRNG I have changed the bit generation procedure so that it takes the following form:

```
1. If reseed_counter > reseed_interval, then return âreseed requiredâ
```

```
2. If (additional_input
 Null), then do
2.1 w = Hash (0x02 || V || additional_input)
2.2 V = (V + w) mod 2seedlen
3. (returned_bits) = Hashgen (requested_number_of_bits, V)
4. and 5.  V = Hash (0x03 || V)
6. reseed_counter = reseed_counter + 1
7. Return (SUCCESS, returned_bits, V, C, reseed_counter)
```

That is, the original steps 4 and 5 have been modified:

```
 4. H = Hash (0x03 || V)
5. V = (V + H + C + reseed_counter) mod 2seedlen
```

Does this simplification make sense?

Problem 5 In the Blockchain used by Bitcoin new blocks are created by miners in a kind of race – any miner can be the author of the next block.

How to prevent the situation that one party with enormous computational power takes over the whole chain? We cannot assume that we change an unfair balance of the computing power.

Problem 6 Choose a model for access control system for IT resources of a company like Uber:

- some (unknown in advance) users provide services
- some (unknown in advance) users buy services
- the company takes care of matching service providers with clients, as well as takes care of the flow of payments

Analyze applicability of standard approaches: ACL, RBAC, ABAC.

Problem 7 Read RFC2693 on SPKI:

https://www.ietf.org/rfc/rfc2693.txt

Understand the mechanism behind this system. There will be a question testing understanding the system behind this RFC document.