University of Asia Pacific

Department of Computer Science and Engineering

Mid Term Examination : Spring-2020

Name: Mahnaz Rafia Islam Registration No: 17101007

Roll No: 07 Year: 4th Semester: 1st Course Code: CSE 407

Course Title: ICT Law, Policy and Ethics Date: 23.08.20

Answer to the question no: 1(a)

At first I will go to the police station and I will fill Ezhar and depending on that an FIR will be launched. If I can show proof police will accept the suspected person and will take him to the front desk magistrate whose formal name is cognizance magistrate withing 24 hrs. Police will Investigate the case. And after Investigation police will provide chargesheet to the cognizance magistrate If police does not receive the case then directly to Court. By magistrate—

Charge Hearing – Either discharge or framing charge.

Framing of charge will be read out to the accused so that he can make defence.

Confession and conviction:

Hearing evidence: If criminal does not agree, evidence needed.

Examination of the accused: Court will ask the criminal if he wants to say anything.

Acquittal: If the case is wrong, the accused person will be acquittal.

Conviction and sentence; If the accused proved guilty then he will get punishment.

Answer to the question no: 1(b)

Digital signature is a key based signature, which is an electronic verification of sender's ~~or~~ personal data or any transaction. It is different from the handwritten signature. It is not the normal signature. It is taken from the Certifying Authority. It has two keys public key and private key.

In the Information Communication Technology Act ~~200~~ 2006, it is mentioned that, in section 17, a digital signature must be taken from the Certifying Authority (CA) to make it secured. Controller allow Certifying Authorities to provide digital signature to its subscribers. Certifying Authority provides ~~license to be~~ Certificate of digital signature to its subscribers. According to section 41, the private key of digital signature must not be shared with others. Only the public key can be shared.

To validate the digital signature -

(i) affixing with the signatory uniquely.
(ii) capable to identify the signatory.
(iii) created in safe manner or using a means under the sole control of the signatory.
(iv) related with the attached data in such a manner that is capable to identify and alteration.

Answer to the question no: 2(a)

"Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfile.

Example: Pdf file, word file, JPG file, .mp3 file, mp4 file etc.

According to section-16 of Information Communication Act 2006, secure electronic record means when any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to a secure electronic record.

Example: By providing digital signature, we can make a electronic record secured. Because only the receiver can view it using the sender's public key.

The scopes and ~~record~~ risks of using electronic records in the present situation of Bangladesh is described below:

Scopes: As Bangladesh is becoming digital Bangladesh using electronic records will be very helpful in the following sections:

(a) Healthcare: Using electronic records will save time for the doctors in healthcare while providing prescription, rather than handwritten prescription.

(b) Bank Sector: Cheque can be issued staying home using electronic record that going to the bank.

(c) E-commerce: To access to the global world, electronic record can be very helpful.

Risks: Also there are many drawbacks of using electronic records in Bangladesh.

In Section 11 of ICT Act 2006 it is mentioned that our government is not ready yet to accept electronic form or records. Besides, there are not internet connection in every corner of Bangladesh yet. Also there is a big

chance of data hack while passing it to the exact receiver. If someone hack an electronic record he can missuse the personal or very secrent information.

Answer to the question no: 2(b)

According to the Section 19 of Information Communication Technology Act 2006 the Cntroller has various functions to follow for the Certifying Authorities. such as -

(a) The Controller must supervise over the activities of the Certifying Authorities.
(b) What type of standards should be maintained by the Certifying Authorities.
(c) Specifying the quality and experience of employees of Certifying Authorities.

(d) Specifying the conditions subject to which the CA shall conduct their business.

(e) If there are any conflict occurs between CA and subscriber, controller will take care of it.

(f) Specifying the form and content of a digital signature certificate that is provided to the CA. (Certifying Authority).

(g) Specifying the form and manner by which accounts shall be maintained by the Certifying Authority.

(h) maintaining database, as mentioned in Section 21, controller to act as repository.

(i) laying down the duties and responsibilities of the Certifying Authority.

(j) Perform any other function under Information Communication Technology Act 2006 or Codes prepared under this act.