Student ID: 20649008
Name: Du Yue

Q1: What is the motivation for proposing the identity-based encryption?

Traditional public key encryption based on digital certificate(CBE) has problems like:
1. The generation of key pairs, the issuing of digital certificates, the publication of the digital certificates, and the management of all these requires a dedicated secure infrastructure.
2. Public Key Inrastructure (PKI) is expensive and complex, and does not scale well to large sizes, and does not easily extend to manage parties' attributes, e.g., their roles and rights.

IBE offers an option in some applications. Users' identifier information instead of digital certificates can be used as public key for encryption or signature verification. As a result, IBE reduces the system complexity and the cost for establishing and managing PKI.

Q2: What are the advantages and disadvantages of the IBE over the traditional certificate-based public key encryption?
Advantages:
1. Eliminate the need for digital certificate and thus certification authorities
2. Simplify the key management in some aspects
3. IBE does not has revocation problem. But CBE has it, and to solve it, user have to check whether public keys have been revoked or not, which slows down the deployment of PKI.

Disadvantages:
1. IBE has "key escrow" property problem. The property might be useful in some situations where user's privacy can possibly be limited. However, in CBE, this key escrow property is not desirable since the "non-repudiation" property is one of the essential requirement of digital signature schemes.

Q3: Can an IBE system be used for signing digital documents? If yes, can the digital signature be used for non-repudiation?
Yes.
No. Because IBE has key escrow property problem which means it is not used for non-repudiation. The use of IBE may be limited to the environment where the PKG is unconditionally trusted.

Q4: Do you think IBE will be widely used? Please justify your conclusion.
Yes.
1. When defining context of pieces of identifier information which used as public key in IBE, it can bring many benefits for users.

2. There is C/C++ implementation of IBE, Stanford and Shamus's library both have implemented IBE scheme. Also, the applications of IBE include IBE email system which provides plug-ins for Outlook, hotmail and Yahoo.