1. 
(a) [1pt] YES - It applies to PK as well.
(b) [1pt] No  (The OTP is the only cryptosystem that isn't subject)
(c) [1pt] Yes
(d) [1pt] Yes
(e) [6pt] 
Using brute force attack both in DES and AES, that is, an
attacker must try every possible key in the entire key space one
by one, and check whether the resulting plaintext obtained from
its corresponding ciphertext is meaningful. And this means that
an attacker needs a way to verify that his guess was correct
- i.e. verifiable plaintext.

For RSA, just guess all key pairs. In fact with the public key you
can generate your own ciphertext.
With big key pairs it might not be practical, but it is possible.

(f) [6pt] 2pt for DES, 2pts for AES, 2pts for RSA

The size of the key space is a factor. By exhaustive key search
in an expected time on the order of $2^{(k-1)}$ operations.
For small RSA keys (512 or below) it is a real problem.
For DES it is a real problem ($2^{55}$ operations required).
For AES, it is more theoretical. ($2^{127}$ operations required assuming
key length of 128bits. Note that the attack against AES can be reduce
to complexity of about $2^{100}$.
In any case though, even if the key space is large, if keys are
derived from passwords, that effectively shrinks the key space
making it a real problem.

(g) [4pt] Need to list only 2. 2pts for each answer.
+ Increase the key size (note that longer keys impose additional costs
e.g. generation, transmission, and storage)
+ Frequently change the key (e.g short key lifetime)
+ Increase the entropy of key (e.g. avoid using weak keys)
+ Use multiple encryptions (e.g. with independent keys)
+ If algorithm supports variable block size, increasing the block
  size often enhances security
+ Choose good passwords, or use a really random key stored on a device
of some kind.
+ Note that changing keys does not help prevent decryption of ciphertext that has already been sent, but it does make the keys less valuable (i.e. guessing the key yields less text), and if the value of the encrypted information goes down with time, that is another benefit.

2.
   a.
   - Floppy disk, USB disk and compact flash memory cards, Hard disk
   - Smart cards
   - Human mind
   - Biometrics
   - Write on a paper
   - RSA security card

   Smart cards or these kinds of devices are resistant to disclosure of the key to malicious software

   b.
   A) Floppy disk, USB disk and compact flash memory cards
      Pros: Portable, Easy to use
      Cons: Can be stolen, limited storage capacity

   B) Biometrics
      Pros: It cannot be duplicated, difficult to forge,
      Cons: Requires special readers such as iris scan, fingerprint scan etc., difficult to revoke/change in case there is a change in the voice (due to illness), finger gets cut etc.

   C) Smart cards
      Pros: Tamper resistant and/or tamper-evident, not vulnerable to even keyboard sniffer, key never leaves the card
      Cons: Costly, requires special readers, if stolen/used then it can be used by others

   D) Human mind
      Pros: Cannot be stolen or sniffed, cannot be stolen/lost
      Cons: Can forget, difficult to remember long keys.

   Grading:
   a. 1 point for each correct category
   b. 4 points each for the advantages and disadvantages of each category mentioned in a.
3.
a)
SSL
Access Control: No
Audit: No
Authentication: Yes (using verify steps)
Confidentiality: Yes (each side using their private key)
Integrity: Yes (If attacker modifies any message then it is discovered either in the verify steps or challenge/response stage.

Note that though it doesn't provide access control directly, the encryption prevent circumvention, through which an attacker might read data in transit that they were not supposed to see. I would accept both yes and no for access control, if suitably explained.

PGP
Access Control: No/Yes
Audit: No/Yes
Authentication: Yes (Using Digital signatures)
Confidentiality: Yes. Encryption with public key and decryption with private key ensures Confidentiality
Integrity: Yes. Digital signatures can take care of integrity of the message.

b)
SSL
Authentication, Confidentialty and integrity hold as long as:
- Persistence of the protections in SSL is only as the data goes over the protected link.
- The connection between the sender and the receiver is maintained.
- The key is valid
- private key is not stolen
- Certificate has not expired/revoked.
- PMKey is not stolen.

PGP
Confidentiality and Integrity holds as long as:
- You have trust in the person who signed the certificate of other persons.
- The certificate may have expired/revoked.
- The owner of the key revokes the key (in case it is stolen or produced a new one).

PGP on the otherhand protects the data, regardless of where it is stored. Once signed and encrypted, the message can move from place to place or be stored on disk while still in protected
C) Weaknesses in SSL:
What: Key distribution using certificates.
Where: In the certificate steps in the SSL

What: PMKey may be cracked and hence then the attacker can hijack the conversation.
Where: Step 3 of the SSL authentication steps.

The main weakness is Phishin Vulnerability
i.e. you may not know that the entity with which you are communicating is really the one you want to be talking with. All you might have to go by is the name, which could be an unnoticeable variant of what you really want.

Weaknesses in PGP:
What: Keys and/or certificates distributed informally with no central authority like Verisign to sign certificates,
Where: Affects security of the mail message.

What: There might be multiple chains and some might lead to different keys for the same person
Where: During Key Distribution in PGP.

What: If you find a chain, how much do you trust it?
Where: During Key Distribution in PGP.

What: Key storage on disk.
Where: If the PGP keys are stored on the disk then it is vulnerable to malicious software.

D) SSL provides key management using a PKI. There is a strict hierarchy with the root as the Certificate Authority. Since it uses the PKI, it is slow but it is secure as long as the CAs are not compromised. Hence SSL has a single point of failure. Hence in terms of security, SSL performs better than PGP. There is no local database of public keys. All the certificates are signed by CA. There is a challenge/response required for Authentication which increases the number of message exchanges. SSL is more complex since it requires using PKI and it has 5 messages to be exchanged for authentication.

PGP provides key management using a Web Of Trust.
There is no such hierarchy in PGP. Since it does not involve the use of PKI, it is faster but its security depends on the number of people in its web of trust. Hence PGP have multiple point of failure. Hence in terms of security, PGP performs well only if the web of trust is not compromised. PGP stores all the public keys locally and refers to it when it wants to send encrypted messages, sign messages etc. All the certificates are signed by people in your web of trust. There is no challenge/response messages since PGP provides no Authentication. PGP is less complex since it stores the public key in the local database and requires no PKI.

Management is easier on SSL because, as commonly used, only the servers are registered with keys, and little communication is needed to distribute those keys. The keys are signed by a CA, whose public keys are embedded in browsers. Subsequent authentication of the user is usually performed in a local manner.

Management of keys is harder for PGP or S/MIME, often requiring the ability to retrieve keys from key servers. Also, because the protections in PGP S/MIME are persistent, it means that even when a key changes, information about the old key still needs to be retained.

Grading:
- a. 1 point for a yes/no for each of the protection with an explanation if "yes".
- b. 2.5 points for PGP and 2.5 points for SSL.
- c. Same as above
- d. Points given if major issues such as Key management, key storage, Trust Hierarchy, Public/Private key cryptography issues.

4. [30pt] 10pts for each strategy. Each strategy needs to have at least

Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. Often hackers imitate the e-mails of legitimate companies to entice people to share personal information. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and social security numbers.

Short-term (10pts): Send out consumer advice:
+ Do not update your important personal information e.g. credit card number, billing info, PIN, usernames, and passwords to a site they connect with by following links in email messages, regardless of how official the site looks.
+ Customer should always go directly to the site using the name for the site they were given when they opened their account, or that appears on their real physical statements.
+ They can bookmark these links if they want.
+ Look out ofr misspelled or poorly written links
+ Watch out suspicious-Looking Links & Pop-Ups' links containing all or part of a real bank's name asking you to submit personal information.
+ Don't use the links in an email to get to the bank web page
+ Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your bank and all card issuers

Mid-term(10pts): Browser plug-ins and updated browser
+ Install a web browser tool bar to help protect you from known phishing fraud websites
  + Display warning messages
  + For example, A browser toolbar that alerts you before you visit a page that's on browser's list of known fraudulent phisher web sites
  + Browser warns you whenever you go to a new domain that you haven't visited.

Extension of infrastructural component to identify phishing? (3pts)
+ Distribution via a set of trusted centers by ensuring that your browser is up to date and security patches are securely applied

What weakness?
+ Browser plugin or toolbar solution is browser dependent.
+ Some toolbars/plugins are trojans themselves

Long-term(10pts):
+ Install and maintain anti-virus software, firewalls, and email filters (SPF record) to reduce some of phishing traffic
+ Employ AI techniques (e.g. KnowledgeBase system) to detect and give warnings to the user, if the software running on the client detects a suspicious activity (either statistical approach or pattern matching)

+ Employ recommendation systems based on the notion of trust
  (The recommendation system is probably one of the most important steps)
+ Obstacles to deployment of the approach?
  o Installation and management of new softwares at thousands of client machines
  o False alarms generated by these phishing detection softwares
  o Evaluation, dissemination & revocation of trust information are not easy