D. computing in Galbraith fields

Correct Answer: A
Explanation:
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as computing in Galois fields, RSA is quite feasible for computer use.
Source: FITES, Philip E., KRATZ, Martin P., Information Systems Security: A Practitioner's Reference, 1993, Van Nostrand Reinhold, page 44.

QUESTION 687
What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

A. Internet Key Exchange (IKE)
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol

Correct Answer: A
Explanation:
The Key management for IPSec is called the Internet Key Exchange (IKE)

Note:
IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.

The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.

IKE--Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. IKE is implemented in accordance with RFC 2409, The Internet Key Exchange.

The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.
IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.)

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:

Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
Allows you to specify a lifetime for the IPSec security association.
Allows encryption keys to change during IPSec sessions.

Allows IPSec to provide anti-replay services.
Permits certification authority (CA) support for a manageable, scalable IPSec implementation.
Allows dynamic authentication of peers.

About ISAKMP
The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME) describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection.

ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management.

About Oakley
The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec
The IETF's IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

IPSec
Internet Key Exchange (IKE)
Data Encryption Standard (DES)
MD5 (HMAC variant)
SHA (HMAC variant)
Authentication Header (AH)
Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services.

For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security."

About SKEME
SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security

models over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability

SKEME's basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.

However, SKEME is not restricted to the use of public keys, but also allows the use of a pre-shared key. This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC) such as Kerberos.

In short, SKEME contains four distinct modes:

Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-Hellman.
A key exchange based on the use of public keys, but without Diffie-Hellman. A key exchange based on the use of a pre-shared key and on Diffie-Hellman. A mechanism of fast rekeying based only on symmetrical algorithms.

In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH.

During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys. These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two peers are also encrypted. If a shared secret already exists, this phase is skipped.
The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie-Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.
The public values or nonces are authenticated during the authentication phase (AUTH), using the secret key established during the SHARE phase.

The messages from these three phases do not necessarily follow the order described above; in actual practice they are combined to minimize the number of exchanged messages.
References used for this question:

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 172).

http://tools.ietf.org/html/rfc4306
http://tools.ietf.org/html/rfc4301
http://en.wikipedia.org/wiki/Internet_Key_Exchange

CISCO ISAKMP and OAKLEY information
CISCO Configuring Internet Key Exchange Protocol
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

QUESTION 688
Which of the following is true about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.

C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Correct Answer: C
Explanation:
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

The following answers are incorrect:

It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).

It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.

It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

References:
MIT http://web.mit.edu/kerberos/Wikipedi
http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

QUESTION 689
Which of the following ASYMMETRIC encryption algorithms is based on the difficulty of FACTORING LARGE NUMBERS?

A. El Gamal
B. Elliptic Curve Cryptosystems (ECCs)
C. RSA
D. International Data Encryption Algorithm (IDEA)

Correct Answer: C
Explanation:
Named after its inventors Ron Rivest , Adi Shamir and Leonard Adleman is based on the difficulty of factoring large prime numbers.

Factoring a number means representing it as the product of prime numbers. Prime numbers, such as 2, 3, 5, 7, 11, and 13, are those numbers that are not evenly divisible by any smaller number, except 1. A non-prime, or composite number, can be written as the product of smaller primes, known as its prime factors. 665, for example is the product of the primes 5, 7, and 19. A number is said to be factored when all of its prime factors are identified. As the size of the number increases, the difficulty of factoring increases rapidly.

The other answers are incorrect because:

El Gamal is based on the discrete logarithms in a finite field. Elliptic Curve Cryptosystems (ECCs) computes discrete logarithms of elliptic curves. International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64 bit blocks of data and is a SYMMETRIC algorithm.

Reference:
Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 638

QUESTION 690
Which of the following can best define the "revocation request grace period"?

A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information

Correct Answer: D
Explanation:
The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.

A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices.
If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

QUESTION 691
What is the primary role of cross certification?

A. Creating trust between different PKIs
B. Build an overall PKI hierarchy
C. set up direct trust to a second root CA
D. Prevent the nullification of user certificates by CA certificate revocation

Correct Answer: A
Explanation:
More and more organizations are setting up their own internal PKIs. When these independent PKIs need to interconnect to allow for secure communication to take place (either between departments or different companies), there must be a way for the two root CAs to trust each other.

These two CAs do not have a CA above them they can both trust, so they must carry out cross certification. A cross certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issued them themselves.

When this is set up, a CA for one company can validate digital certificates from the other company and vice versa.