1 Security aspect and the Techniques used

Security Aspect	Techniques Used
P - Privacy / Confidentiality	encryption/decryption (symmetric/asymmetric)
A - Authentication / Identification	challenge-response protocols
I - Integrity of data / data origin	message digests, hash functions
N - Non-Repudiation	digital signatures

2 Public Key Crypto Systems (PKCS)

2.1 First Class of PKCS - RSA algorithm-based

2.1.1 System Setup

1. Generate two "large" and "good" primes p and q of comparable size.
2. $n = pq$ and $\Phi(n) = (p-1)(q-1)$. $\Phi(n)$ =cardinality of the set $\{j | 1 \leq j \leq n, gcd(j, n) = 1\}$.

2.1.2 User Setup

1. Choose random integer e such that $gcd(e, \Phi(n)) = 1$.
2. Compute the multiplicative inverse d of e modulo $\Phi(n)$ i.e. such that $e.d = 1(mod\, \Phi(n))$.
3. Publish (e, n) as the public key of the user and keep (d, n) as the private key with the user.

2.1.3 Usage

Encryption / Decryption

$$\boxed{\text{cipher } c \equiv m^e (mod\, n)}$$
$$\boxed{\text{message } m \equiv c^d (mod\, n)}$$

Signing / Verification

$$\boxed{\text{sign : } c \equiv m^d (mod\, n)}$$
$$\boxed{\text{verify : } m \equiv c^e (mod\, n)}$$

2.1.4 Strengths

1. **RSA primitive** - Given n and c, determine m. There does not seem to exist a polynomial time algorithm for this.

2. **Factor primitive** - Factoring n into the consituent large primes p and q does not seem to be solvable in polynomial time. The best algorithm known is a sub-exponential time algorithm.

2.2 Second Class of PKCS - Discrete Logarithm Problem - based

2.2.1 System Setup

1. Select a large prime p and a generator g for the cyclic group Z_p^*.

2.2.2 User Setup

1. Choose random α such that $1 \leq \alpha \leq p-1$.
2. Compute $a \equiv g^{\alpha}(mod\, p)$.
3. Publish a as the public key of the user and keep α as the private key of the user.

2.2.3 Usage

Encryption

1. Choose random k and compute $s \equiv g^k(mod\, p)$.
2. Compute $r \equiv^k (mod\, p)$.
3. Compute $c \equiv rm(mod\, p)$.
4. Send the pair (s, c).

Decryption

1. Compute $r = s^{\alpha}$.
2. Compute $m \equiv cr^{-1}(mod\, p)$.

2.2.4 Strengths

Given a and g such that $a \equiv g^x$, finding x in polynomial steps (i.e. $O(|G|)$ is not known.

3 Public Key Infrastructure (PKI)

Reference Links
http://www.ietf.org/html.charters/pkix-charter.html
http://www.pki-page.org/
http://csrc.nist.gov/pki/
http://home.xcert.com/~marcnarc/PKI/References.htm