Department of Computer Science and Engineering
I Sem. M.Tech(Computer Science and Information Security)
Advanced Cryptography CSE 5171
Formula Sheet

RSA Digital Signature Scheme

$S = M^d \bmod n$
Verification $M' = S^e \bmod n$
Is M congruent to M'?

ElGamal Digital Signature Scheme

first signature $S1 = e1^r \bmod p$
second point $e2 = e1^d \bmod p$
second signature $S2 = (M - d \times S1) \times r^{-1} \bmod (p - 1)$
$V1 = e1^M \bmod p$
$V2 = e2^{S1} \times S1^{S2} \bmod p$
Is V1 =V2 ?

Schnorr Digital Signature Scheme

Signature $S1 = h(M | e1^r \bmod p)$
Signature $S2 = r + d \times S1 \bmod q$
Verification $V = h(M | e1^{S2} e2^{-S1} \bmod p)$
Is S1 congruent to V?

Digital Signature Standard (DSS)

$e1 = e0^{(p-1)/q} \bmod p$
$e2 = e1^d \bmod p$
Signature $S1 = (e1^r \bmod p) \bmod q$
Signature $S2 = (h(M) + d\ S1)r^{-1} \bmod q$
Verification $V = [(e1^{h(M)} S2^{-1} e2^{S1\ S2^{-1}}) \bmod p] \bmod q$

The ECDSS scheme

$P(u, v) = r \times e1\ (\ldots, \ldots)$
Second point $e2 = d \times e1(\ldots, \ldots)$
Signature $S1 = u \bmod q$
Signature $S2 = (h(M) + d \times S1)\ r^{-1} \bmod q$.
$A = h(M)\ S2^{-1} \bmod q$ and $B = S2^{-1}\ S1 \bmod q$
Third Point $T(x, y) = A \times e1\ (\ldots, \ldots) + B \times e2(\ldots, \ldots)$
Is x congruent to S1 mod q?

Blind Signature

Blinded message $B = M \times b^e \bmod n$
Signature on the blind version of the message $S_b = B^d \bmod n$
Signature is $S = S_b\ b^{-1} \bmod n$

Chaum and van Antwerpen Undeniable signature

Signature $s = m^k \pmod p$
Challenge $c = s^a (g^k)^b \pmod p$
Response $r = c^{k-1}$
Check whether $r = m^a g^b \pmod p$

Fiat-Shamir Protocol

$v = s^2 \bmod n$
$x = r^2 \bmod n$
$y = rs^c \bmod n$
Is y^2 congruent to xv^c ?

Feige-Fiat-Shamir Protocol

[s1, s2, …, sk] - a vector of private keys
[v1, v2, …, vk]- a vector of public keys
a vector of challenges (c1, c2, …, ck)
$x = r^2 \pmod n$

$vi = (si^2)^{-1} \bmod n$
$y = (rs1^{e1}\ s2^{e2}\ s1^{e3}\ \ldots\ sk^{ek}) \bmod n$
Is $y^2 v1^{c1}\ v2^{c2}\ v1^{c3}\ \ldots\ Vk^{ck}$ congruent to x

Guillou-Quisquater Protocol

$s^e \times v = 1 \bmod n$
$x = r^e \pmod n$
$y = rs^c \bmod n$
Is x congruent to $y^e\ v^c$