Security

a) Never use the same $k$ twice. Otherwise

\[ s_1 = k^{-1}(h(w_1) - x r) \mod (p-1) \]
\[ s_2 = k^{-1}(h(w_2) - x r) \mod (p-1) \]

\[ (s_1 - s_2)k = (h(w_1) - h(w_2)) \mod (p-1) \]

\[ k = (s_1 - s_2)^{-1}(h(w_1) - h(w_2)) \mod (p-1) \]

provided $(s_1 - s_2)^{-1} \mod (p-1)$ exists.

Once $k$ is known, $x$ can be computed from $(k)$.

b) We cannot forge a signature on a message $w$ as follows.

Select any pair $(u, v)$ s.t. $\gcd(v, p-1) = 1$

Compute

\[ r = a^u v \equiv a^{u+xv} \mod p \]
\[ s = -rv^{-1} \mod (p-1) \]

Then $(r, s)$ is a valid signature on

$w = s - t \mod (p-1)$

Proof. (Ex)

Avoid this attack by using hash $h(w)$ instead of $w$. 

c) Verification step requiring \( t \leq r \leq p - 1 \).

If this check is omitted, \( R \) can sign messages of his choice provided he has one valid signature.

Suppose \((r, s)\) is a valid signature on message \( m \).

\( R \) selects message \( m' \) and computes

\[ h(m') \quad \text{and} \quad r' = h(m') (h(m))^{-1} \quad \text{mod} \ (p - 1) \]

provided \((h(m))^{-1} \quad \text{mod} \ (p - 1)\) exists.

Further

\[ s' = s \cdot r' \quad \text{mod} \ (p - 1) \]

\( r' \) such that \( r' = r \cdot u \ (\text{mod} \ (p - 1)) \)

\[ r' = r \ (\text{mod} \ p) \]

(by the CRT)

The pair \((r', s')\) is a signature on \( m' \), which would accepted without checking \( t \leq r' \leq p - 1 \).

\( \exists \)
8.4. Public Key Infrastructure (PKI)

Most important components:
- Certificate issuance
- Certificate revocation
- Key backup/recovery/update
- Time stamping

PKI enables:
- Secure communication
- Access control
- Privacy architecture

Example: SSL (secure socket layer)
A (client) wants to purchase something from B (server).

Client A

Server B

\[ y = e_{PB}(MS) \]

\[ MS = d_{PB}(y) \]

\[ (K_{1}, K_{2}) = h(MS) \]

\[ (K_{1}, K_{2}) = h(MS) \]
K₁ is used to authenticate data by a MAC(K₁)

K₂ is used for encryption/decryption

(e.g. DES, triple DES, AES, others)

Note: A may not even have a public.

Needed in e-commerce: not the identity of D, but the verification of the credit card no.