PKCS1 Signatures

Derek Mayo

PKCS1 Signatures

- Similar to PKCS1 used for public key encryption
- Signature to verify sender identity and untampered message

Variable Definitions

- n - t-bit long RSA modulus, t is a multiple of 8
- e - encryption exponent
- m - a message
- H - collision resistant hash function the outputs of which are h bits long, h also a multiple of 8 and h < t - 88

Structure

- D is a member of $\mathbb{Z}_n$
- Signature takes *e*th root of D to get σ
- Verification takes σ^e and checks if all of the above fields are present

Attack

- Attacker finds 3 messages m1, m2, and m3 such that

$$H(m1) = a, \quad H(m2) = b \quad H(m3) = ab$$

- Submits messages m1 and m2 then uses the information from those to forge a signature for m3

Sources

- A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup