CS-406
Cryptography and Network Security

Digital Signatures

Yathansh Kathuria 140050021

Aditi Laddha 130050026

April 26, 2017

INTRODUCTION

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. Digital signatures are a standard element of most cryptographic protocol suites

.

BASICS OF DIGITAL SIGNATURE:

A digital signature scheme is a triple of probabilistic polynomial time algorithms, (G, S, V), satisfying:

- ◇ G (key-generator) generates a public key, pk, and a corresponding private key, sk, on input 1^n, where n is the security parameter.
- ◇ S (signing) returns a tag, t, on the inputs: the private key, sk, and a string, x.
- ◇ V (verifying) outputs accepted or rejected on the inputs: the public key, pk, a string, x, and a tag, t.

For correctness, S and V must satisfy:

$$Pr[(pk, sk) \leftarrow G(1^n), V(pk, x, S(sk, x)) = accepted] = 1$$

A digital signature scheme is secure if for every non-uniform probabilistic polynomial time adversary, A:

$$Pr[(pk, sk) \leftarrow G(1^n), (x, t) \leftarrow A^S(pk, 1^n), x \notin Q, V(pk, x, t) = accepted] < negl(n)$$

wherewhere $A^{S(sk,.)}$ denotes that A has access to the oracle, S(sk, $\cdot$), and Q denotes the set of the queries on S made by A, which knows the public key, pk, and the security parameter, n. Note that we require any adversary cannot directly query the string, x, on S.

DIGITAL SIGNATURE SCHEMES:

1. Lamport signature

It is a one-time signature scheme, built from cryptographically secure one-way function; usually a cryptographic hash function is used.

2. Merkle signature scheme

The Merkle signature scheme is a digital signature scheme based on hash trees (also called Merkle trees) and one-time signatures such as the Lamport signature scheme. It is an alternative to traditional digital signatures such as the Digital Signature Algorithm or RSA. It is believed to be resistant against quantum computer algorithms

3. Digital Signature Algorithm

This is the most commonly used Digital Signature scheme and uses a new key per-message.

4. Schnorr Signature Scheme

the security of Schnorr Signature Scheme is based on the intractability of certain discrete logarithm problems. The Schnorr signature is considered the simplest digital signature scheme to be provably secure in a random oracle model. It is efficient and generates short signatures.

SCOPE OF PROJECT

In this project we have built a Schnorr Signature Scheme implemented in a server client model. All the messages sent by the server are signed via the server's private key and the client accepts the message only if the signature gets verified via the server's public key. Moreover all the messages sent by the server are encrypted using RSA encryption (using the pubic key of the client to whom the message is being sent). The sementics of Schnorr's scheme are as follows:

.

◇ **Key Generation:**

1)Select 2 large primes such that :

$$p = q * t + 1$$

2)Select h such that 1 <h <p-1 and set

$$g = h^t mod p$$

if g is 1 than re chose h and repeat.

3)Chose x such that 0<x<q. This x is the signer's private key

4)Set:

$$y = g^x mod p$$

This y along with p,q,g are the signer's public key.

Note : the group (of order q) generated by g is a subgroup of Zp^x and is called the Schnorr group. Dicrete Log Assumption holds true on this group

◇ **Signing Algorithm**

1)Chose a random number k such that 0<k<q

2)Let:

$$r = g^k mod p$$

3)Let:

$$e = H(r \parallel M)$$

4)Let :

$$s = k - x * e$$

5)The pair (s,e) is the signature

◇ **Verifying Algorithm**

1)Calculate:

$$r_v = g^s y^e mod p$$

2)Calculate:

$$e_v = H(r_v \parallel M)$$

3)Signature is valid if e and ev are equal otherwise it is invalid

UNDENIABLE SIGNATURE

Undeniable signature is a digital signature scheme and implementation invented by David Chaum and Hans van Antwerpen in 1989. In this scheme, a signer possessing a private key can publish a signature of a messages. However, the signature reveals nothing to a recipient/verifier of the message and signature without taking part in either of two interactive protocols:

- Confirmation protocol, which confirms that a candidate is a valid signature of the message issued by the signer, identified by the public key.
- Disavowal protocol, which confirms that a candidate is not a valid signature of the message issued by the signer.

The motivation for the scheme is to allow the signer to determine to whom he verifies or disavows a signature, and it is the interactive nature of the protocols that allows this; i.e., the result of each protocol is non-transferable. However, if there were only a confirmation protocol, there would be no way to distinguish between: the case that the signature is not a valid signature by the signer at issue, and the case that the signature was a valid signature by the signer at issue, but the signer now chooses not to take part in verification. The disavowal protocol provides an interactive (i.e., non-transferable) proof of the former case.