RSA Encryption and Decryption

Kevin Liao and Josh Smith

November 28, 2016

1 Introduction

Intro goes here.

2 Key Pair Generation

We follow the FIPS Digital Signature Standard [1] to generate key pairs.

2.1 Pseudorandom Number Generator

In order to generate random primes, it is important that we use a cryptographically secure pseudorandom number generator. We decide to use the UNIX-based special file `/dev/random`, which generates high-quality pseudorandom numbers that are well-suited for key generation.

The semantics for `/dev/random` vary based on the operating system. In Linux, `/dev/random` is generated from entropy created by keystrokes, mouse movements, IDE timings, and other kernel processes. In macOS, `/dev/random` data is generated using the Yarrow-160 algorithm, which is a cryptographic pseudorandom number generator. Yarrow-160 outputs random bits using a combination of the SHA1 hash function and three-key triple-DES.

We believe `/dev/random`, as prescribed, is sufficient for our purposes, but the entropy pool can be further improved using specialized programs or hardware random number generators.

2.2 Criteria for Key Pairs

The key pair for RSA consists of the public key (n, e) and the private key (n, d). The RSA modulus n is the product of two distinct prime numbers p and q. RSA's security rests on the primality and secrecy of p and q, as well as the secrecy of the private exponent d. The methodology for generating these parameters varies based on the desired number of bits of security and the desired quality of primes. However, the following desideratum must hold true for all methods.

2.2.1 Public Exponent e

1. The public verification exponent e must be selected prior to generating the primes p and q, and the private signature exponent d.

2. The public verification exponent e must be an odd positive integer such that $2^{16} < e < 2^{256}$.

It is immaterial whether or not e is a fixed value or a random value, as long as it satisfies constraint 2 above. For simplicity, we fix $e = 2^{16} + 1 = 65537$.

2.3 Primes p and q

¡++¿

2.4 Private exponent d

3 Generation of Probable Primes with Conditions Based on Auxiliary Probable Primes

Uhm.

4 Encryption and Decryption

References

[1] PUB FIPS. 186-4. *Digital Signature Standard (DSS)*, 2013.