COMP6453 Tutorial Week 7

1 OpenSSL

Use OpenSSL to view the Moodle (moodle.telt.unsw.edu.au) certificate. Answer the following questions:

1. What is the RSA public key algorithm? Analyse its components.
2. What is the signature algorithm? Analyse its components.
3. Try viewing other website certificates and answer questions 1 and 2.

Hint: OpenSSL Command Line Utilities

2 Random Self Reducibility of Discrete Log

We would like the security of cryptographic algorithms to be based on problems which are hard on *average*. Many problems are hard only in the worst case, such as subset sum, which is not optimal for cryptographic purposes. We will show if the discrete log problem is hard in the worst case (which we believe is true), then it must be hard on average.

Let G be a fixed cyclic group of order q and g be a fixed generator of G. Suppose $\mathcal{A}$ is an efficient adversary with the following property: if $\mu \in G$ is chosen at random, then $Pr[A(\mu) = Dlog_g(\mu)] = \epsilon$. Show there is an efficient algorithm $\mathcal{B}$ with the following property: for all $\mu \in G$, algorithm $\mathcal{B}$ outputs $dlog_g(\mu)$ with probability ϵ.

3 Wiener's Attack

The Wiener's attack, named after cryptologist Michael J. Wiener, is a type of cryptographic attack against RSA. The attack uses the continued fraction method to expose the private key d when d is small.

Recall the RSA setup:

- Choose large primes p and q, compute $n = qp$
- Compute $\phi(n) = (q-1)(p-1)$
- Choose e, $1 < e < \phi(n)$ such that $gcd(e, \phi(n)) = 1$
- Use Extended Euclidean Algorithm, compute d with $ed \equiv 1 \mod (\phi(n))$
- Delete $q, p, \phi(n)$
- Public key (n, e)
- Private key d

Note that: It is infeasible to compute d from (n, e) without knowing either q or p.

Wiener's theorem

Let $n = qp$ with $q < p < 2q$. Let $\frac{1}{3}$ and given n, e with $ed \equiv 1 \mod (\phi(n))$, the adversary can efficiently recover d.

The key idea of Wiener's attack is the observation that $\frac{e}{n} \approx \frac{k}{d}$ for some integer k. You can read more and play around with the given Python code from here.

Some observations on RSA

Note that the left-hand side of the approximation is constructed entirely from public information.

Wiener's attack works by expanding $\frac{e}{n}$ to a continued fraction and iterating through the terms to check various approximations of $\frac{k}{d}$. For example:

$$\frac{e}{n} = \frac{17993}{90581} = \frac{5}{1 + \frac{1}{29 + \cdots + \frac{1}{3}}} = [0, 5, 29, 4, 3, 2, 4, 3]$$