Modern Cryptography

600.442

Lecture #13

Dr. Christopher Pappacena

Fall 2013

Private Key Cryptography

- Private key cryptography can be used to provide secure, authenticated communication.

- Its use depends on the communcants being able to agree on a shared secret key.

- How do the communicants decide on their shared key?

Three Challenges

- Key Distribution: How do communicants establish their private keys?

- Key Management: How do individuals communicate with many other people?

- Transient Communcations: How do individuals with no prior relationship communicate securely?

Key Distribution

In a *closed* environment (e.g. a company), key distribution can be handled *physically*:

- Each new person, when hired, is issued keys to communicate with other employees.
- Unwieldy, since a new employee needs n keys if the company employs n people.
- Current employees also need to update their key lists as new employees are enrolled.
- These keys must all be stored securely.

Key Distribution Centers

In a closed environment, a *key distribution center* (KDC) can eliminate lots of these problems.

- Each employee, when hired, is issued private keys (encryption and authentication) to communicate securely with the KDC.

- When employees want to communicate securely, they contact the KDC to receive a *session key*.

Basic KDC Protocol

- When Alice wants to communicate securely with Bob, she contacts the KDC.

- The KDC generates a session key k and sends Alice $(\mathsf{Enc}_A(k), \mathsf{Enc}_B(k))$, where A and B are Alice and Bob's keys.

- Alice decrypts $\mathsf{Enc}_A(k)$ to obtain k and uses it to encrypt her message to Bob.

- Alice sends Bob $\mathsf{Enc}_B(k)$ and $\mathsf{Enc}_k(m)$ where m is her message.

- Authentication can be accomplished in the same fashion.

KDCs – Pros and Cons

- Each employee only needs to securely store a single key, making key distribution and management easier for individuals.

- The KDC has access to everyone's key, making it a target for adversaries.

- The KDC is a single point of failure for secure communication throughout the company – if it goes down, secure communication becomes impossible.

- KDCs can be replicated to increase resiliency, but this introduces more targets for adversaries.

In practice, KDCs are used to provide enterprise-level secure communications.

But they do not address the problem of enabling *transient* secure communication:

> *How can two people communicate securely over a public channel without having previously established a secret key and without access to a private channel to establish this secret?*

Until the mid 1970's, accomplishing this was considered *impossible*.

Diffie-Hellman and the Public Key Revolution

In 1976, Diffie and Hellman published a paper titled "New Directions in Cryptography".

In it, they introduced three public-key primitives:

- Public-Key Encryption
- Digital Signatures
- Interactive Key Exchange

Diffie and Hellman presented a solution to the last of these, now known as the *Diffie-Hellman Key Exchange*.

Original Diffie-Hellman Key Exchange

- Alice chooses a large prime p and a *generator** g.

- Alice chooses $x \leftarrow \{1, \ldots, p-1\}$ and computes $A = g^x \pmod{p}$.

- Alice sends p, g, and A to Bob.

- Bob chooses $y \leftarrow \{1, \ldots, p-1\}$, computes $B = g^y \pmod{p}$, and sends B to Alice.

- Alice and Bob both know $g^{xy} = A^y = B^x \pmod{p}$.

*We'll define this later.

Diffie and Hellman's work preceded modern notions of cryptographic security so they did not provide a formal proof of security.

They did observe that, for the key exchange to be secure, *at a minimum* the following problem must be hard:

The Discrete Logarithm Problem: Given p, g, and $A = g^x \pmod{p}$, determine x.

This is because an eavesdropper sees both $A = g^x$ and $B = g^y$ during the exchange.

We'll discuss this problem in more generality later.

Rivest-Shamir-Adleman and ElGamal

- In 1978, Rivest, Shamir, and Adleman presented solutions to public-key encryption and digital signatures.

- RSA encryption remains the most widely-used public-key algorithm in the world.

- In 1985, ElGamal created public-key encryption and digital signature algorithms based on the same underlying problem as the Diffie-Hellman key exchange.

In short, Diffie and Hellman revolutionized cryptography, created the field of public-key cryptography, and came very close to providing solutions to all of the basic problems that they introduced.

Public-key algorithms are built using operations that are easy to implement, but hard to undo:

- Given integers g and x and a prime p it is easy to compute $g^x \pmod{p}$, but given $g^x \pmod{p}$ it is difficult to determine x.

  This dichotomy is the heart of the Diffie-Hellman key exchange and El Gamal encryption and digital signatures.

- It is easy to multiply two primes togther, but difficult to factor an integer which is the product of two large primes.

  This dichotomy is the heart of RSA encryption and digitial signatures.

To understand these problems, we need to do some number theory.

Elementary Number Theory

Division Algorithm: Let a be an integer and let b be a positive integer. Then there exist integers q, r, with $0 \leq r < b$, such that $a = bq + r$.

This just says we can divide a by b and get a remainder which is less than b.

If a and b are nonnegative integers, then their *greatest common divisor* (GCD) is the largest integer c which divides both a and b. We write $c = (a, b)$ for the GCD of a and b.

Example: $(12, 16) = 4$.

Lemma: Let $c = (a, b)$. Then there exist integers x, y such that

$$ax + by = c,$$

and c is the smallest positive integer which can be written in this form.

Example: $12 \cdot (-1) + 16 \cdot 1 = 4$, so $x = -1$ and $y = 1$ works. Taking $x = 15$ and $y = -11$ also works.

We write $\|a\|$ for the number of bits in a, which is the relevant quantity for algorithmic complexity.

Given integers a and b, we can compute $c = (a, b)$ and integers x, y such that $c = ax + by$ in time polynomial in $\max(\|a\|, \|b\|)$ using the *extended Euclidean algorithm*

Modular Arithmetic

Let N be a positive integer. We write $a = b$ (mod N), or $a \equiv b$ (mod N), if $a - b$ is divisible by N.

This is equivalent to saying that a and b have the same remainder when divided by N.

Example: $345678722566563473 = 544574598645293 73$ (mod 100).

Reduction modulo N respects addition, subtraction, and multiplication: if $a = a'$ (mod N) and $b = b'$ (mod N), then $a \pm b = a' \pm b'$ (mod N) and $ab = a'b'$ (mod N).

In general, we *cannot* divide modulo N: $3 \cdot 2 = 15 \cdot 2$ (mod 24) but $15 \neq 3$ (mod 24).

If a is an integer, then there exists a *unique* integer r with $0 \leq r \leq N-1$ such that $a = r \pmod{N}$ – namely, the remainder when we divide a by N.

We write $\mathbb{Z}_N$ for $\{0, \ldots, N-1\}$ with arithmetic defined modulo N. The fact that we can add, subtract, and multiply essentially says that $\mathbb{Z}_N$ is a *ring*.

An important computational fact is that we can reduce modulo N "as we go" when doing computations.

Addition and multiplication in $\mathbb{Z}_N$ can be computed in polynomial time in $\|N\|$.

Units in $\mathbb{Z}_N$

An element u of $\mathbb{Z}_N$ is called a *unit* if it has a multiplicative inverse v, so that $uv = 1 \pmod{N}$. The set of units in $\mathbb{Z}_N$ is written $\mathbb{Z}_N^*$.

Example: 7 is a unit modulo 10 since $7 \cdot 3 = 1 \pmod{10}$. In fact, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.

Proposition: u is a unit modulo N if and only if $(u, N) = 1$.

Proof: If $(u, N) = 1$, write $ux + Ny = 1$. Then $x = u^{-1} \pmod{N}$.

Groups

A *group* G is a set with a binary operation $\circ$ satisfying three axioms:

- Associativity: $g \circ (h \circ k) = (g \circ h) \circ k$.

- Identity: There exists an element e such that $e \circ g = g \circ e = g$ for all g.

- Inverse: For every g, there exists h such that $g \circ h = h \circ g = e$. We write $h = g^{-1}$.

If $g \circ h = h \circ g$ for all $g, h \in G$, we call G an *abelian group*. We will *only* work with finite abelian groups.

Examples

- The set of integers modulo N, $\mathbb{Z}_N$, with operation addition, is an abelian group.

  The identity element is 0 and the inverse of a is $N - a$:

  $$a + (N - a) = N = 0 \pmod{N}.$$

- The set of units modulo N, $\mathbb{Z}_N^*$, with operation multiplication, is an abelian group.

  The identity element is 1 and the fact that every element has an inverse follows from the definition of “unit”.