

Encryption 2

Tom Chothia

Computer Security: Lecture 3

Last Lecture:

- Symmetric Key Encryption Ciphers
 - Frequency Analysis
 - One time pads
 - AES, DES and 3-DES
- Block cipher modes
- Truecrypt

Advanced Encryption Standard (AES)

- AES is a state-of-the-art block cipher.
- It works on blocks of 128-bits.
- It generates 10 round keys from a single 128-bit key.
- It uses one permutation: ShiftRows and three substitutions SubBytes, MixColumns, AddRoundKey.

Block Cipher Modes



Original



ECB



CBC

Frequency Analysis

- Without CBC, frequency analysis can be used on each block.
- Without probabilistic encryption, frequency analysis can be used on each message.
- Without padding, frequency analysis can be used on the length of messages.

This Lecture

- Diffie Helleman key exchange
- Public Key Encryption
 - RSA
 - Signing
 - Combining public and symmetric key encryption

Some History

Before cheap powerful computers, unbreakable encryption was almost impossible.

Governments wanted to read the codes of others.

They could control the export of these machines.

When IBM designed DES they could get it weakened.

- Cipher machines looked like this:



Some History

During 1970-1990 all that changed.

Personal computers could do anything a cipher machine could do.

University academics worked on encryption with the aim of making it available to everyone.



The Key Problem

- These encryption schemes work well. AES is effectively unbreakable with a “long enough key”.
- The problem is how do you get the key in the first place?

Public Key Encryption

- Public key encryption helps (but doesn't solve) this problem.
- The idea of public key encryption is that you have two keys:
 - one for encryption
 - and another for decryption.
- The encryption key is made public, the decryption key is always secret.

Diffie-Hellman

- Diffie-Hellman is a widely used key agreement protocol.
- It relies on some number theory:
 - $a \bmod b = n$ where for some “m” : $a = m.b + n$
- The protocol uses two public parameters
 - generator “g” (often 160 bits long)
 - prime “p” (often 1024 bits long)

Diffie-Hellman

- Alice and Bob pick random numbers r_A and r_B and find “ $t_A = g^{r_A} \text{ mod } p$ ” and “ $t_B = g^{r_B} \text{ mod } p$ ”
- The protocol just exchanges these numbers:
 1. $A \rightarrow B : t_A$
 2. $B \rightarrow A : t_B$
- “Alice” calculates “ $t_A^{r_A} \text{ mod } p$ ” and “Bob” “ $t_A^{r_B} \text{ mod } p$ ”
this is the key:
 - $K = g^{r_A r_B} \text{ mod } p$

Diffie-Hellman

- An observer cannot work out r_A and r_B from t_A and t_B therefore the attacker cannot calculate the key
- So we have a “**Good Key**” but know nothing about the participants.
- **We did not need to share any keys at the start, therefore this is a very powerful protocol.**
- In practice: use DH to set up a secure channel, then use something else to authenticate the person at the other end.

Elgamal

- Elgamal, is Diffie-Hellmen turned into a public key scheme. It uses a fix g & p
- “Alice” picks r_A as her *private key*
& “ $t_A = g^{r_A} \text{ mod } p$ ” is *the public key*.
- To encrypt message “M”, Bob picks r_B finds
and sends $(g^{r_B} \text{ mod } p, M \cdot t_A^{r_B})$

RSA

- RSA is the most popular public key cipher.
 - More efficient than Elgamal, and allows for signing.
- It uses two large primes p & q .
We set $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$
- Pick random
 - e such that $1 \leq e \leq \phi(n)$ and e and $\phi(n)$ are co-prime.
 - d such that $d \cdot e \bmod \phi(n) = 1$

The public key is (e, n) and the private key is (d, n)

RSA

- To encrypt a message, turn it into numbers “m” that are less than “n”
- To encrypt as cipher text c do:
$$c = m^e \bmod n$$
- To decrypt a cipher text c as a message m do:
$$m = c^d \bmod n$$

Some More History

- These ciphers make encryption pretty much unbreakable.
- They made encryption available to everyone and the Internet, as we know it, possible
- But Diffie, Rivest, etc. weren't the first. At the British intelligence service GCHQ:
 - James Ellis invented the concept of public keys in the 1960's
 - Malcolm J. Williamson invented DH in 1974
 - Clifford Cocks invented RSA in 1973
- But GCHQ distributed their keys via embassies, so never used it.

Message Length Limit

- RSA cannot encrypt messages longer than the key size.
 - RSA is also slow, so CBC is very slow.

Answer: Encrypt an AES key with the RSA Key, then encrypt the message with AES

- $E_{RSA}(M) = E_{K_{RSA}}(K_{AES}), E_{K_{AES}}(M)$

Signatures

- Using RSA $E_{\text{pub}}(D_{\text{priv}}(M)) = M$
- This can be used to sign messages.
- Sign a message with the private key and this can be verified with the public key.
- Any real crypto suite will not just encrypt with a public key, as this can be used to trick people into decrypting.
- Usually sign just the hash of the message.

Elliptic curve crypto

- Public key encryption based on elliptic curves.
- Functionally very like RSA, but more efficient.
- No full security proof, but recommended by NSA.
- Becoming the most popular web public key encryption system.

Review

- Diffie Helleman key exchange
- Public Key Encryption
 - RSA
 - Signing
 - Combining public and symmetric key encryption

Further Reading

- Mark Ryan's note on symmetric encrypts and public key encryption.
 - Linked to from the website.
- Volker's Cryptology module
- Bruce Schneier: Applied Cryptography
- The Code Book, by Simon Singh.

Recommended Key Lengths

- See <http://www.keylength.com/>

Introduction to Java and Object Oriented Programming

What is a computer program?

Any program

- Instructions to a computer
- Data plus algorithm
- Takes in input carries out a process and generates output
- May be divided into smaller chunks (i.e. functions and modules)

An object-oriented program

- ❖ Made up of “*objects*”
- ❖ An object has
 - ❖ State called *fields*,
 - ❖ Behaviours called *methods*
- ❖ An OO program achieves things through interactions between objects
 - ❖ One object calls another (passes a message)

How do we define the characteristics of an object?

- In your program, you define “**Classes**”.
- You use “**Classes**” to create “**Objects**”.
- You retain references to “**Objects**”
- You call “**Methods**” to perform computation.
- You use “**Methods**” to manipulate data held in “**Fields**” within an Object.

Public/Private

- The key word `public` makes a field or method accessible outside the class.
- `private` stops all direct access.
- It's good practice to use `private` for parts of the class you might want to change.

Constructors

- Constructors are used to make a new object.
- Declare a constructor by:

```
public <className> (arguments) {  
    ...  
}
```

Objects and Methods

- Always think about running methods on objects.
 - e.g. given Number objects “x” and “y”
 - `x.add(y)` is more OO than `x = add(x, y)`
- Why write methods against objects?
- How do you decide which class should contain a method?

Static Methods.

- But not all methods in Java are called on objects,... what's going on here?
- Sometimes methods are required that don't run against a specific object.
 - Initial program method ("main")
 - Factory methods
 - Methods that are not object specific
- Any methods or fields that are not related to a specific object are declared as "static".

Static Field

- A static field is one that is the same for all objects. E.g. static pi.
- A static method is one that is the same for all objects.
- Static methods can't refer to none static fields. Why?
- Static methods don't need to be called on a particular objects. (Classname.method())

Next Lecture

- More Java
- How to do encryption in Java.
- How to use a “keystore” to look after your keys.