**Cryptography Part 3**

The log4j vulnerability

**What is it?**

A vulnerability in log4j that allows users to create injection attacks on computers.

**How does it work?**

It basically allows a user to force a machine into string interpolation. They can then use placeholder variables (${yourVarHere}) to make calls to a remote server and the program will evaluate whatever is sent in response. That means that any program that uses this may be able to be hacked by simple input from the user.

**Why is it important?**

On a broad level, the log4shell vulnerability is critical because log4j is used by millions of java programs. Java is one of the most popular programming languages in the world and has been for a long time, so it’s a huge issue, potentially affecting millions of companies and individuals.

When the vulnerability is exploited with JNDI, (a java api that provides naming and directory functionality to applications), attackers can pretty much run whatever code they want on the host machine.

**How was it fixed?**

The log4shell vulnerability was patched in updates by the Apache development team. However, when using certain versions of log4j, the vulnerability is still a major issue. JNDI may not be used safely on log4j version 2.16.0