# Lab 6: PKI with JSSE

**Översikt**
Skapa en krypterad http-anslutning i java.
Den här labben är mycket mer teoretisk än de andra. Fokus ligger på få ut den nödvändiga informationen från vanliga referenskällor. Det är viktigt att du förstår exakt hur din kod fungerar, framför allt alla keywords och argument.

I den här labben är det viktigt att du kan svara på ALLA frågor och att du vet vad ALLA keywords betyder utan att använda en cheat sheet.

Skapa ett certifikat med hjälp ett ett keytool, och sätt upp en ny keystore i din projektmapp. Det kan vara så att det redan finns en keystore i din hemmamapp, men det är antagligen ingen bra ide att modifiera den. Skapa sedan en server som väntar på en HTTPS-anslutning. Servern behöver bara skicka tillbaka “Hello World!” för att visa att den fungerar eftersom det är bara att hantera den som en vanlig socket efter det. Efter det så ska du bara behöva koppla upp dig med en webläsare (firefox eller chrome) och efter att ha accepterat det självsignerade certifikatet så ska du kunna koppla upp dig säkert.

**Specifika krav**
1. SSLSockets **måste** användas.
2. Din kod måste vara **ordentligt** kommenterad.
3. Du måste förstå **alla** keyword i koden.

**Tips:**
JSSE reference guide är VÄLDIGT hjälpsam för alla stegen i labben.
Om du använder dig av eclipse sa måste certifikatet placeras i projektmappen och inte i SRC eller BIN.

**References:**
Cryptographic Right Answers
https://gist.github.com/tqbf/be58d2d39690c3b366ad
JSSE guide
http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html
Bild på TLS handshake med förklaringar
https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/tls/tls.html

**Frågor:**

- Vad är PKI?
- Vad löser PKI för problem?
- Vad innehåller ett certifikat? Förklara alla fält.
- Hur valideras ett certifikat? Vilka algoritmer används på vilka fält och i vilken ordning?
- Hur levereras root-certifikaten till din dator?
- Vad är en trust chain?
- Är det säkert att lagrad lösenorden till certifikaten till din dator? Varför/Varför inte?
- Förklara HELA handshaket.
- Explain how the PKI work.
- När i handshaket används symmetriskt kryptering?
- När används asymmetriskt kryptering?

**Keywords:**

X.509, TLS/SSL, RSA, Private key, Public key, cipher suite, HTTPS, MD5/SHA, AES

**Bonus**

Sätt upp en tor hidden service. Den måste inte göra något mer än att printa “Hello World!”. Kom ihåg att den måste fungera under labben så planera för att det kan ta en stund att sätta upp. Det är medvetet tunna instruktioner.

**Frågor:**

Varför är TOR så säkert?
Hur kan någon råka avslöja vem de är eller bli spårade? Nämn åtminstone två olika sätt.