# MAT 301 Finals Checklist

- Do you know:

  1. **[Groups]:** Groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$, and how to compute the Euler Totient Function $\phi(N)$, given the factorization of $N$?
  2. **[Euclid and Extended Euclid]:** how to find gcd's and inverses by hand using (Extended) Euclid?
  3. **[Exponentiation]:** how to compute $b^a \pmod{N}$ given $b, a$ and $N$?
  4. **[Root Finding]:** how to solve for $x$ in the equation $x^a = b \pmod{N}$?
  5. [**Fermat and Euler**]: Do you know Fermat's and Euler's theorems?
  6. **[Caesar, Vigenere and the One-time Pad]:** Make sure you know how these work, and what their weaknesses are.
  7. **[The Asymptotic Notation]:** What does the $O(\cdot)$ notation mean? Do you know the running times of the algorithms presented in class?
  8. **[RSA]:** How does the RSA Cryptosystem work? I will focus on the underlying mathematics.
  9. [**Primality Testing**]: Do you know the Fermat Primality Test? Do you know what Fermat Witnesses and Liars are?
  10. [**Discrete Logarithms and the Diffie-Hellman Protocol**]: Make sure you understand these well.

  **After Midterm:**

  11. [**El Gamal Public key Encryption Scheme**]: You may be asked to describe the encryption scheme, so you should know how it works.
  12. [**Chinese Remainder Theorem**]: Work out examples to make sure you understand CRT very well.
  13. [**Zero Knowledge**]: Make sure you know the protocols for proving that a number is a square mod $N$, and the protocol for proving knowledge of discrete logarithms, both of which were presented in class.
  14. [**Secret Sharing**]: Make sure you understand the basic $t$-out-of-$N$ threshold secret sharing, and also the more advanced examples from problem set 5 and the practice final. Learn also how threshold secret sharing is used in conjunction with the El Gamal encryption scheme to achieve threshold decryption.
  15. [**Malleability / Man in the Middle Attacks**]: Do you know the man-in-the-middle attack against the Diffie-Hellman protocol, and the malleability attacks against RSA and El Gamal?

- There will be 5 or 6 problems in the final.

- You will have 3 hours to solve these problems. You can bring a double-sided A4 "cheat sheet".