Some desirable properties of a cryptographic system

- **Confidentiality:** Information is kept secret from all but authorized parties
- **Integrity:** Messages have not been modified in transit
- **Message Authentication:** The sender of the message is authentic
- **Nonrepudiation:** The sender cannot deny the creation of the message
- **Unconditionally secure:** The system cannot be broken, even with infinite computational resources. (Tough/impossible to implement)
- **Kerckhoff's Principle:** A cryptosystem should be secure when the attacker knows all the details of the encryption and decryption algorithms but does not know the secret key.

What approaches have we seen in support of encryption and decryption?

- Use symmetric key system like AES-GCM (or AES w/ HMAC) for

  Confidentiality, Integrity, Authentication

  Super efficient, but requires Alice & Bob have shared, secret symmetric key

- Can use Public Key Cryptography like DHKE to exchange symmetric key
  - PKC is a profound and super-cool concept!
  - To avoid MITM attacks, Alice & Bob need to sign key exchange messages
  - Depends upon Alice & Bob's public credentials being valid
  - How do you stop Oscar from spoofing these?

- Web servers register with a *Certificate Authoritiy*
  - CAs sign the web server's credentials contained in the certificate
  - How do you trust the CA's signature?
  - CA's credentials are written into operating system!

Not all cryptography is about message sharing

- Cryptographic hash functions support integrity
- Digital signatures support authentication and nonrepudiation
- These are the main ideas that make blockchains function!

Some of the mathematical tools we've used

- Modular arithmetic
- $GF(2^8) = \mathbb{Z}[x]/p(x)$ in AES
- Euclidean Algorithm (and EEA) for computing $\gcd(a, b)$ and $a^{-1} \mod m$
- The Square-and-Multiply algorithm makes computing $a^k \mod m$ very efficient even for *huge* k and m
- Solving the Discrete Log $\alpha^x \equiv \beta \mod p$ can be really hard
- **All of our systems can be broken with unlimited time!**
  There are only finitely many possible solutions!
- Security depends upon the number of possibilities being astronomical and there being no known underlying structure that gives a shortcut!