PostSkill:-

Key Generation Techniques:

1. **Symmetric Keys:**
   - **Random Generation:** Keys are created using secure random number generators, ensuring they can't be easily guessed.
   - **Password-Based:** Keys can also come from passwords using special functions to make them more secure.
2. **Asymmetric Keys:**
   - **Prime Numbers:** Keys are made using large prime numbers, as in RSA.
   - **Elliptic Curves:** Keys are created based on points on curves, offering strong security with smaller keys.

Strength of AES Keys:

1. **128-bit Key:**
   - Strong enough for most uses, requiring a huge number of tries to break (2^128).
2. **192-bit Key:**
   - Even stronger, used when extra security is needed.
3. **256-bit Key:**
   - The strongest option, used for highly sensitive information.

Key Management and Storage:

1. **Key Lifecycle:**
   - **Generation:** Keys should be made securely with strong methods.
   - **Distribution:** Share keys safely using secure protocols.
   - **Rotation:** Change keys regularly to keep them secure.
   - **Revocation:** If a key is compromised, stop using it immediately and update the system.