Checksum Verification

1. Algorithm Cipher

A collision within a hashing algorithm spells trouble. Freeman law specified that a collision could allow a hacker to trick a computer system (What is the best hashing algorithm? 2022). Cybercriminals use weak algorithms to crack encryption methods. Some methods used to hack through encryption are Brute Force, Rainbow Table, and Birthday Attacks (What is the best hashing algorithm? 2022). Therefore, selecting the correct methodology is vital.

I am recommending the use of SHA3-256.

2. Justification

First, it is essential to understand that development will occur with Java. Additionally, the project has specified the use of java.security.MessageDigest library. This limited the consideration of all possible algorithms to MD2, MD5, SHA (1, 224, 256, 384, 512/224, 512/256), and SHA3 (224, 256, 384, 512) (Java security standard algorithm names).

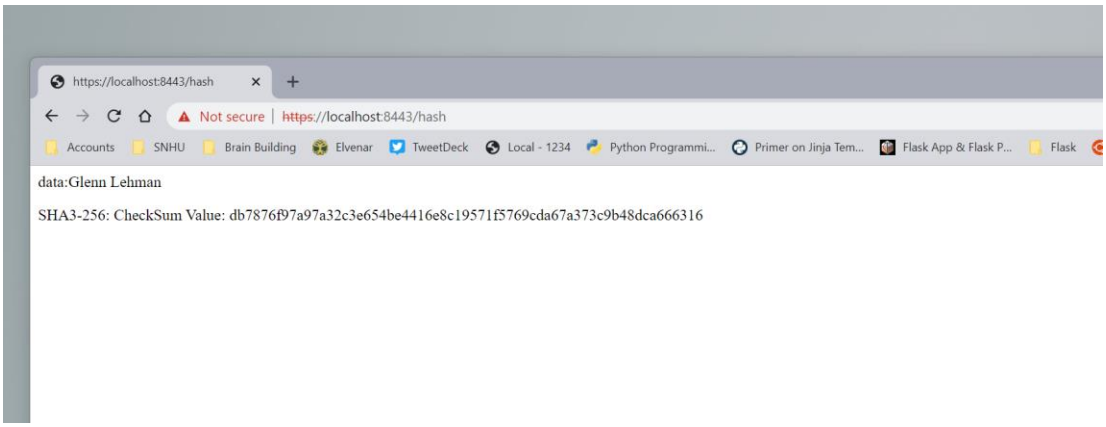
Both MD2 and MD5 have demonstrated a history of collisions. According to Bruce Schneier, MD5 was cracked in 2005 with a collision attack (Projects, 2005). MD5 replaced MD2 after documenting collision issues related to the compression algorithm inside MD2 (Knudsen & Mathiassen, 2005).

SHA, which is SHA-2, would be sufficient based on most use cases. Today the cryptocurrency world commonly utilizes SHA-256. Unfortunately, SHA-2 is vulnerable to a length of extension attack. This pushes the best option to SHA-3 is considered highly secure and currently published as the official recommended crypto standard (Nakov, 2018).

3. Generate Checksum

```
@RestController
class ServerController{

    @RequestMapping("/hash")
    public String myHash(){
        String data = "Glenn Lehman";
        String hashed_data;

        hashed_data = makeMyHash(data);


        return "<p>data:"+data+hashed_data;

    }

    public String makeMyHash(String data){

                //create an instance of the MessageDigest by using the getInstance() method with the SHA3-
256 algorithm
                MessageDigest obj = null;
                try {
                        obj = MessageDigest.getInstance("SHA3-256");
                } catch (NoSuchAlgorithmException e) {
                        // TODO Auto-generated catch block
                        e.printStackTrace();
                }

                obj.update(data.getBytes());
            //use the digest() method for computing the message digest
            byte[] byteArray = obj.digest();

            //convert the byte array in to Hex String format
            StringBuffer hexData = new StringBuffer();

            for (int i = 0; i < byteArray.length; i++) {
                hexData.append(Integer.toHexString(0xFF & byteArray[i]));
            }

             return "<p><p>SHA3-256: CheckSum Value: "+hexData.toString();
    }
```

4. Verification



Hash collisions explained. Freeman Law. (2022, October 4). Retrieved November 24, 2022, from https://freemanlaw.com/hash-collisions-explained/

Java security standard algorithm names. (n.d.). Retrieved November 24, 2022, from https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html

Knudsen, L. R., & Mathiassen, J. E. (2005, February 1). *Preimage and collision attacks on MD2: Proceedings of the 12th International Conference on Fast Software Encryption*. Guide Proceedings. Retrieved November 24, 2022, from https://dl.acm.org/doi/10.1007/11502760_17

Nakov, S. (2018, November). *Secure hash algorithms*. Secure Hash Algorithms - Practical Cryptography for Developers. Retrieved November 24, 2022, from https://cryptobook.nakov.com/cryptographic-hash-functions/secure-hash-algorithms

Projects, C. to W. (2005, February 16). *Chinese researchers crack major U.S. government algorithm used in digital signatures*. Wikinews, the free news source. Retrieved November 24, 2022, from https://en.wikinews.org/wiki/Chinese_researchers_crack_major_U.S._government_algorithm_used_in_digital_signatures

What is the best hashing algorithm? Code Signing Store. (2022, April 7). Retrieved November 24, 2022, from https://codesigningstore.com/what-is-the-best-hashing-algorithm