Student: Tania Diaz
Date: 09/14/2025
Course: CIST-2881-D1
Assignment: ASSIGNMENT: GOST Hash Function

1. Launch your browser of choice.
2. Navigate to https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf.
3. Read the article and take notes on the characteristics of the function and how it works. Don't be concerned if you can't understand the entire algorithm; focus on the process, especially inputs and outputs
4. Per the article, what is a collision attack?

A collision attack is when two different messages end up giving the same hash value. That means the hash function can't tell them apart, which is a big security problem.

5. Per the article, how does GOST handle collision attacks?

The article shows that GOST has some weaknesses. It was supposed to be strong, but researchers found ways to create collisions faster than expected. They used tricks like working with messages that look the same on both sides (symmetric) and then applied math attacks. In the end, they could find collisions in GOST with less work than the full strength should need.

6. Describe the birthday paradox referred to in the article.

The birthday paradox is the idea that in a group of just 23 people, there's already a 50% chance two share the same birthday. For hash functions, this means you don't need to test all possible outputs to find a collision , you only need about the square root of the total number

7. How can the birthday paradox be used to limit the number of possibilities offered by the hash function?

Instead of needing to try all 2^n outputs, the birthday paradox shows you only need about 2^(n/2) tries to find a collision. That cuts the work in half (on the power scale). In the article, they use this to explain why finding collisions in GOST is easier than it should be.

8. Open another tab in your browser and navigate to https://www.splunk.com/en_us/blog/learn/triple-des-data-encryption-standard.html
9. Read the article.
10. What similarities can you determine between GOST and DES?

Both GOST and DES are symmetric block cipher algorithms. This means they use the same secret key for encryption and decryption, and they process data in fixed-size blocks. Both use multiple rounds of substitution and permutation to transform the plaintext into ciphertext, which makes it harder for attackers to break the encryption.

11. Describe any advantages of using one over the other.

Advantages of one over the other:

DES / Triple DES: Triple DES improves on DES by applying the DES algorithm three times with different keys, making it much more secure than single DES. It's good for compatibility and works on older systems.

GOST: GOST uses a larger block size and key length, which can make it stronger against brute-force attacks compared to the original DES.

12. Why was DES created and where was it first used? Is it still in use today?

Why DES was created and where it was first used:

DES (Data Encryption Standard) was created in 1977 to provide a standard method for encrypting data securely. It was widely adopted in the 1980s and 1990s for financial transactions, government communications, and other industries needing secure data.

Is DES still in use today?

Single DES is considered insecure today due to its short 56-bit key. Triple DES (3DES), which applies DES three times with different keys, was used for extra security, but it is now being phased out and replaced by more modern algorithms like AES (Advanced Encryption Standard).