HASHED PASSWORD CRACKER SIMULATION

GROUP TY58

21.Riya Lanjewar
22.Prachi Lasurkar
35.Manas Kadam
42.Pranav Modhave

PROJECT OVERVIEW

- Overview: Methods to test password security by cracking hashes.

Dictionary Attack

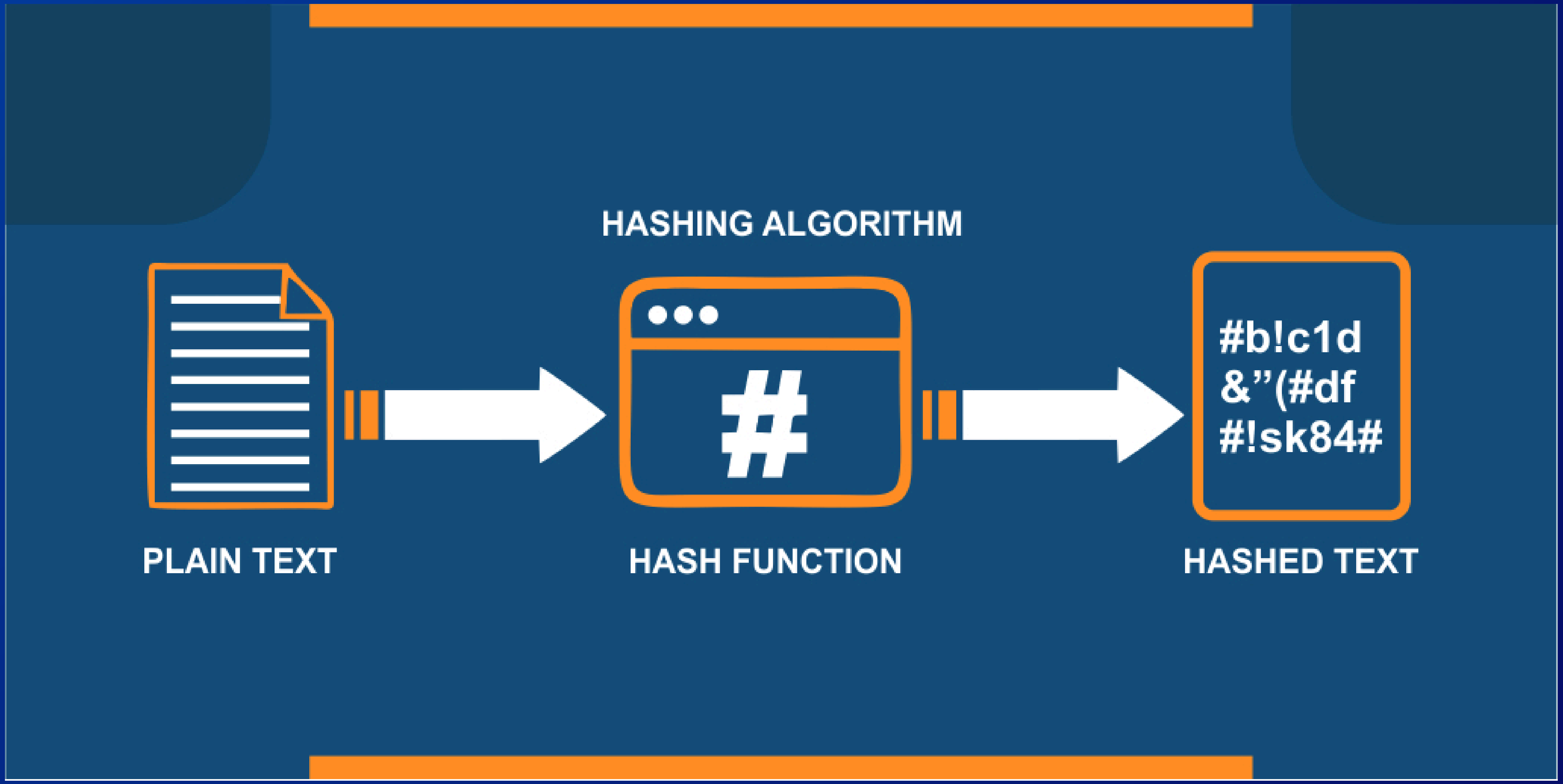
Brute-Force Attack

Mask-Based Attack

HASHING ALGORITHMS

- Hashing: Converts data (like passwords) to fixed-size "hashes" for secure storage.
- MD5: 128-bit, now outdated due to security flaws.
- SHA-1: 160-bit, insecure for modern needs.
- SHA-256: 256-bit, secure and widely used.

SHA-1


HASHING ALGORITHM
#b!c1d
&"(#df
#!sk84#
PLAIN TEXT
HASH FUNCTION
HASHED TEXT

MD5 ALGORITHM

The MD5 algorithm's working process involves padding, appending length, initializing variables, processing in 512-bit blocks, and producing the final hash.

1. **Padding the Input:** The first step in the MD5 algorithm involves padding the input message so its length (in bits) is congruent to 448 modulo 512. This is done by appending a single '1' bit followed by enough '0' bits to reach the required length, ensuring the total message length is a multiple of 512 bits.
2. **Appending the Length:** After padding, the length of the original message (before padding) is appended as a 64-bit value.
3. **Initializing Variables:** MD5 uses four 32-bit variables, which are initialized to specific constants. These variables, often denoted as A, B, C, and D, are set to the following values in hexadecimal:
4. A = 0x67452301,B = 0xefcdab89,C = 0x98badcfe,D = 0x10325476
5. Processing in 512-bit Blocks: The padded message is processed in chunks of 512-bit blocks, each divided into sixteen 32-bit words.
6. **Main Loop**
7. The core of the MD5 algorithm involves four non-linear functions (F, G, H, and I) and four rounds of transformation. Each function takes three 32-bit words as input and produces a 32-bit output.
8. **Producing the Final Hash**After all the 512-bit blocks have been processed, the final hash value is produced by concatenating the variables A, B, C, and D. The resulting 128-bit value is the MD5 hash of the input message.

METHODOLOGY

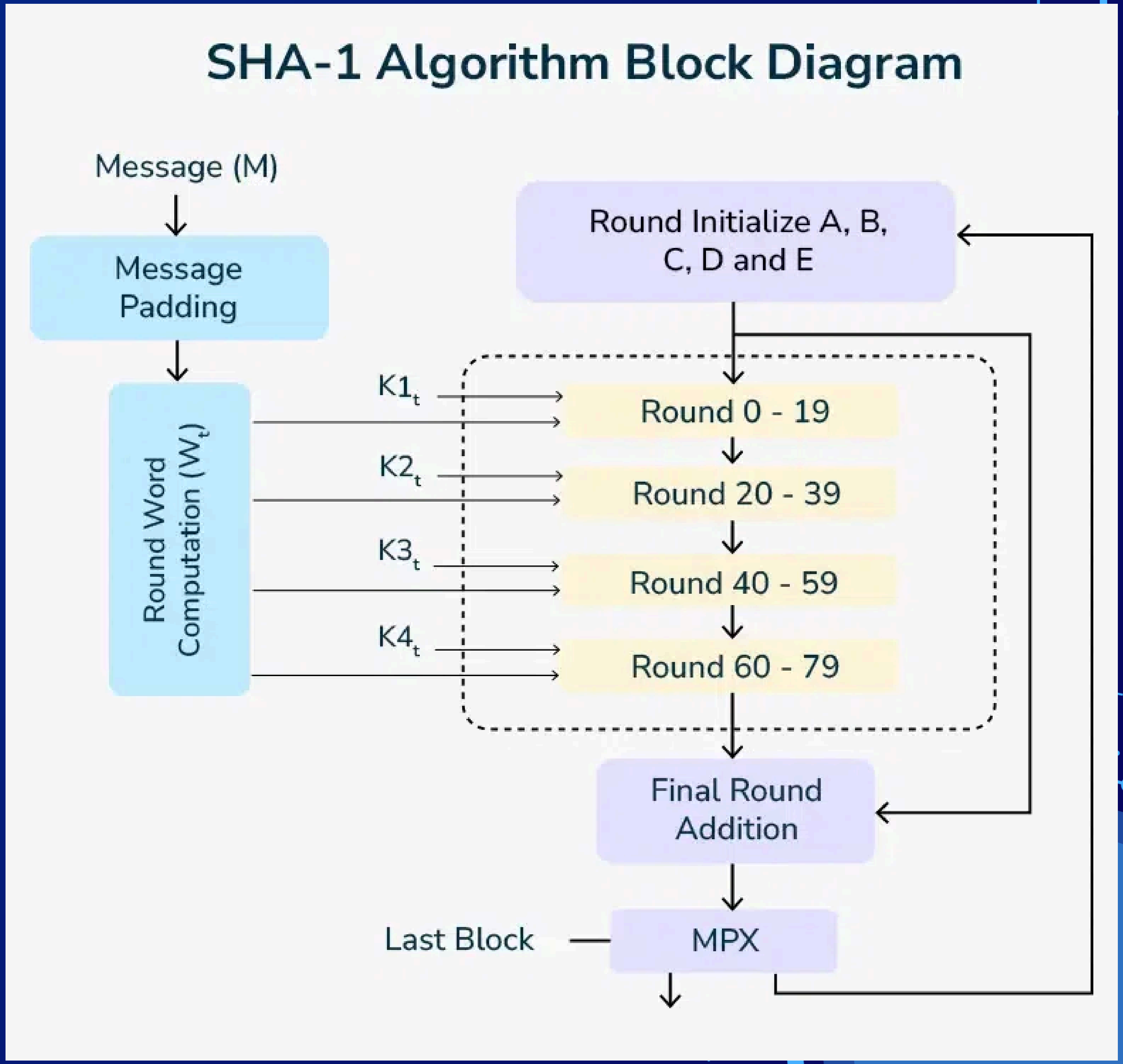
- INPUT : THE PROCESS STARTS WITH THE INPUT MESSAGE MMM.

- MESSAGE PADDING: THE MESSAGE IS PADDED TO MEET THE LENGTH REQUIREMENTS.

- WORD COMPUTATION: THE PADDED MESSAGE IS DIVIDED INTO BLOCKS AND FURTHER INTO WORDS, WHICH ARE EXPANDED FOR USE IN THE ROUNDS.INITIAL HASH VALUES ARE SET.

- ROUND PROCESSING: THE MAIN LOOP PERFORMS 80 ROUNDS OF COMPUTATION USING THE MESSAGE WORDS AND ROUND CONSTANTS.

- FINAL ADDITION: THE RESULTS FROM THE ROUNDS ARE ADDED TO THE INITIAL HASH VALUES.
- OUTPUT : THE FINAL MESSAGE DIGEST IS PRODUCED.



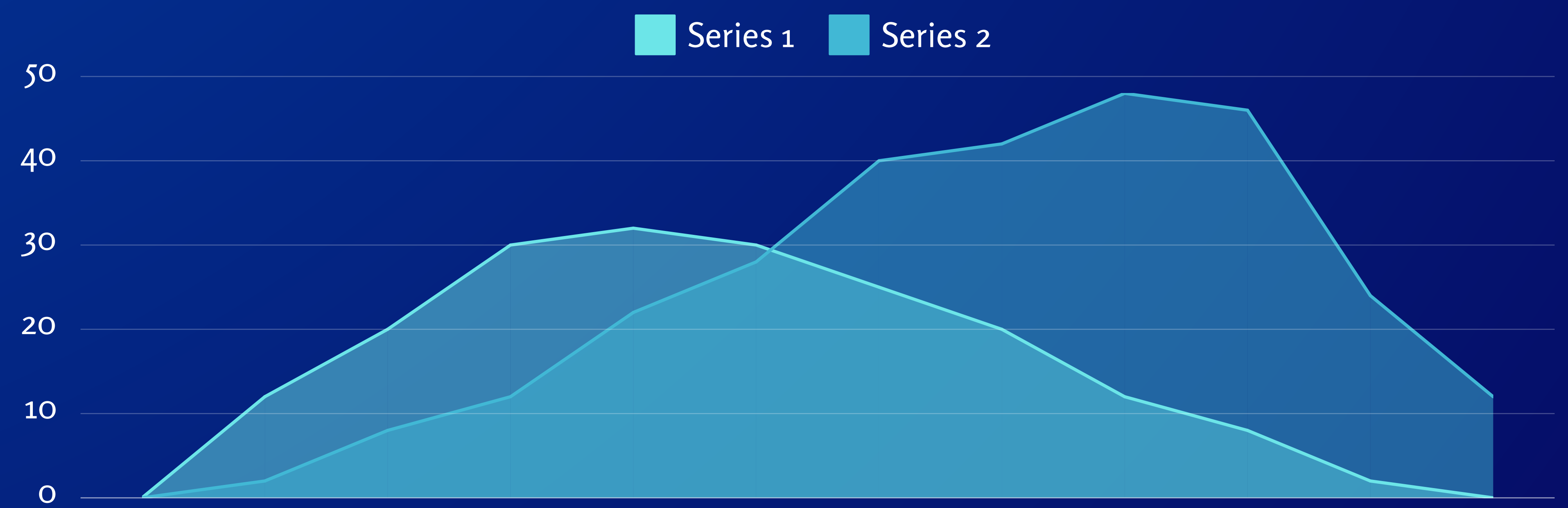
SHA-1 Algorithm Block Diagram

ATTACK TECHNIQUES

- Dictionary Attack: Uses a wordlist to find matching hashes.

- Brute-Force Attack: Tries all possible character combinations.

- Mask-Based Attack: Uses a defined pattern (e.g., LLDD).



PARALLELIZATION AND EFFICIENCY

- Multithreading: Uses ThreadPoolExecutor for concurrent guesses.
- Benefits:

  Faster brute-force and mask-based attacks.

  Improved performance with larger search spaces

USER INTERACTION & CONCLUSION

- User Interaction:
- Choose to hash a password or crack a hash.
- Select between dictionary, brute-force, or mask-based attacks.

- Conclusion: Highlights the importance of strong passwords.

THANK YOU