INTERNAL KNOWLEDGE BRIEFING REPORT
Generated on: 06-12-2025 23:40

EXECUTIVE SUMMARY:

This presentation introduces modern symmetric-key block ciphers, defining them as algorithms that encrypt/

KEY TAKEAWAYS:

*   **Modern Block Ciphers:** Encrypt/decrypt fixed-size blocks (n-bits) using a fixed-size key (k-bits). Comm
*   **Substitution vs. Transposition:** Modern block ciphers need to be designed as substitution ciphers to re
*   **Block Ciphers as Permutation Groups:**
    *   **Full-size Key Transposition Cipher:** Transposes bits, modeled as n-object permutation with n! tables
    *   **Full-size Key Substitution Cipher:** Substitutes bits, modeled as permutation of `2^n!` objects. Key si
    *   **Partial-size Key Ciphers:** Actual ciphers like DES use smaller keys (e.g., 56-bit for 64-bit block) com
*   **Keyless Ciphers (Building Blocks):**
    *   **P-boxes (Permutation Boxes):** Transpose bits.
        *   **Straight P-box:** n inputs, n outputs (invertible).
        *   **Compression P-box:** n inputs, m outputs (m < n, non-invertible).
        *   **Expansion P-box:** n inputs, m outputs (m > n, non-invertible).
    *   **S-boxes (Substitution Boxes):** Miniature substitution units (m x n). Modern block ciphers typically us
*   **Other Components:** Exclusive-OR (XOR), Circular Shift, Swap (special case of circular shift), Split, an
*   **Product Ciphers:** Combine substitution, permutation, and other components.
    *   **Diffusion:** Spreads the influence of a single plaintext bit change over many ciphertext bits.
    *   **Confusion:** Hides the relationship between the ciphertext and the key.
    *   Achieved through iterated rounds, each using a key generated by a key schedule.
*   **Classes of Product Ciphers:**
    *   **Feistel Ciphers:** Can use a mix of self-invertible, invertible, and non-invertible components, achievin
    *   **Non-Feistel Ciphers:** Use only invertible components, requiring explicit inverse components for decr
*   **Security:** Modern block ciphers are designed to resist most attacks possible in classical ciphers.

COMPARATIVE TABLE / DETAILS:

Topic	Page Number
Title Slide (Course & Instructor)	1
Modern Block Ciphers (Definition)	2
Modern Block Ciphers (Diagram)	3
Modern Block Ciphers (Message Handling)	4
Substitution or Transposition (Design)	5
Substitution or Transposition (Resistance)	6
Block Ciphers as Permutation Groups	7
Full-Size Key Transposition Block Ciphers	8
Full-Size Key Transposition Example	9
Full-Size Key Transposition Example (Diagram)	10
Full-Size Key Substitution Block Ciphers	11
Key Sizes Comparison (Question)	12
Key Sizes Comparison (Answer)	13
Permutation Groups (Cascaded Operations)	14
Partial-Size Key Ciphers	15
Partial-Size Key Ciphers (Group Property)	16
Keyless Ciphers (P-boxes & S-boxes)	17
Components of a Modern Block Cipher	18
Three Types of P-boxes (Diagram)	19
Possible Mappings of a Straight P-Box (Diagram)	20
Straight P-Box Details & Example	21