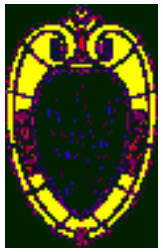


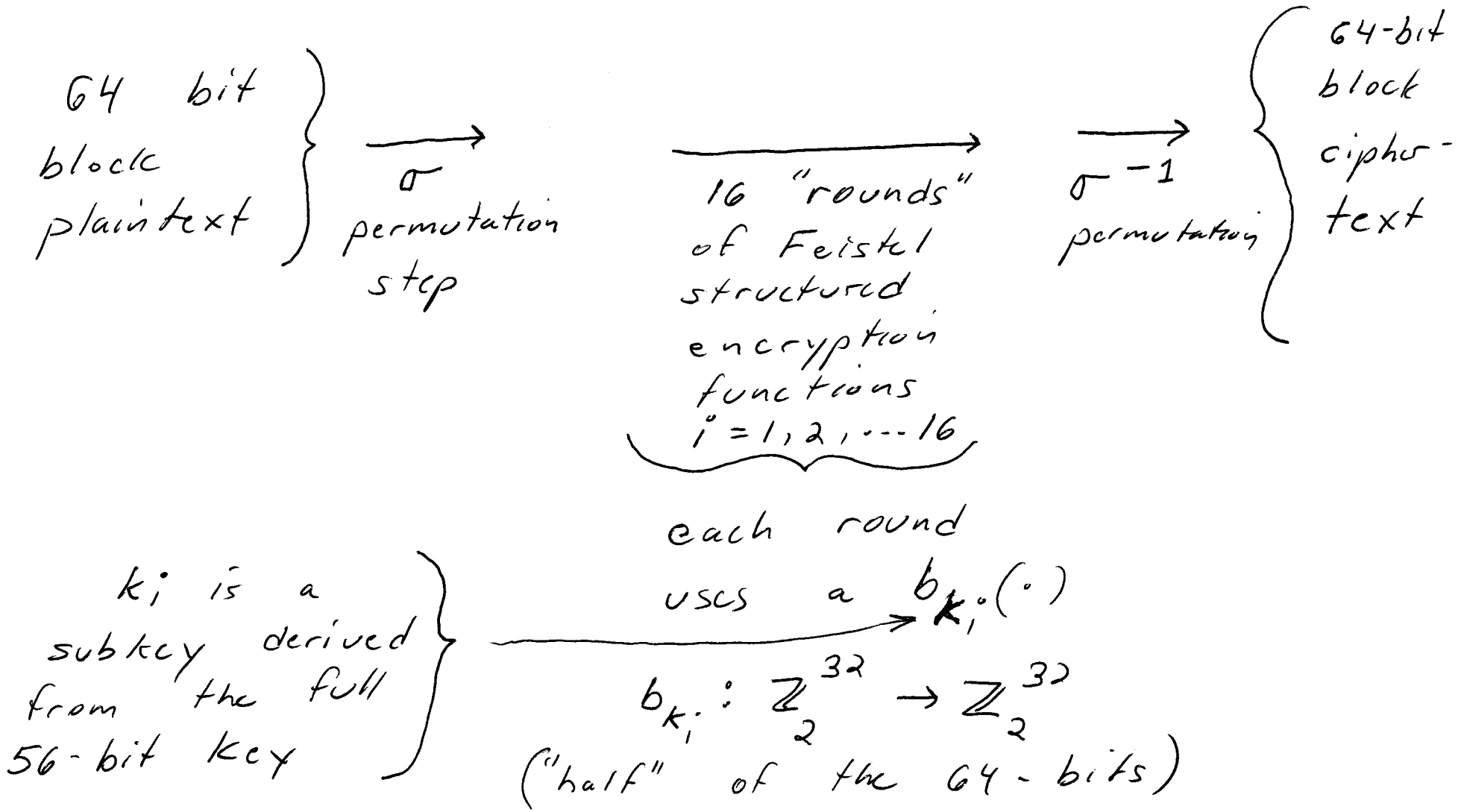
CS/ECE/Math 435
Introduction to Cryptography

Professor Chris DeMarco
Department of Electrical & Computer Engineering
University of Wisconsin-Madison

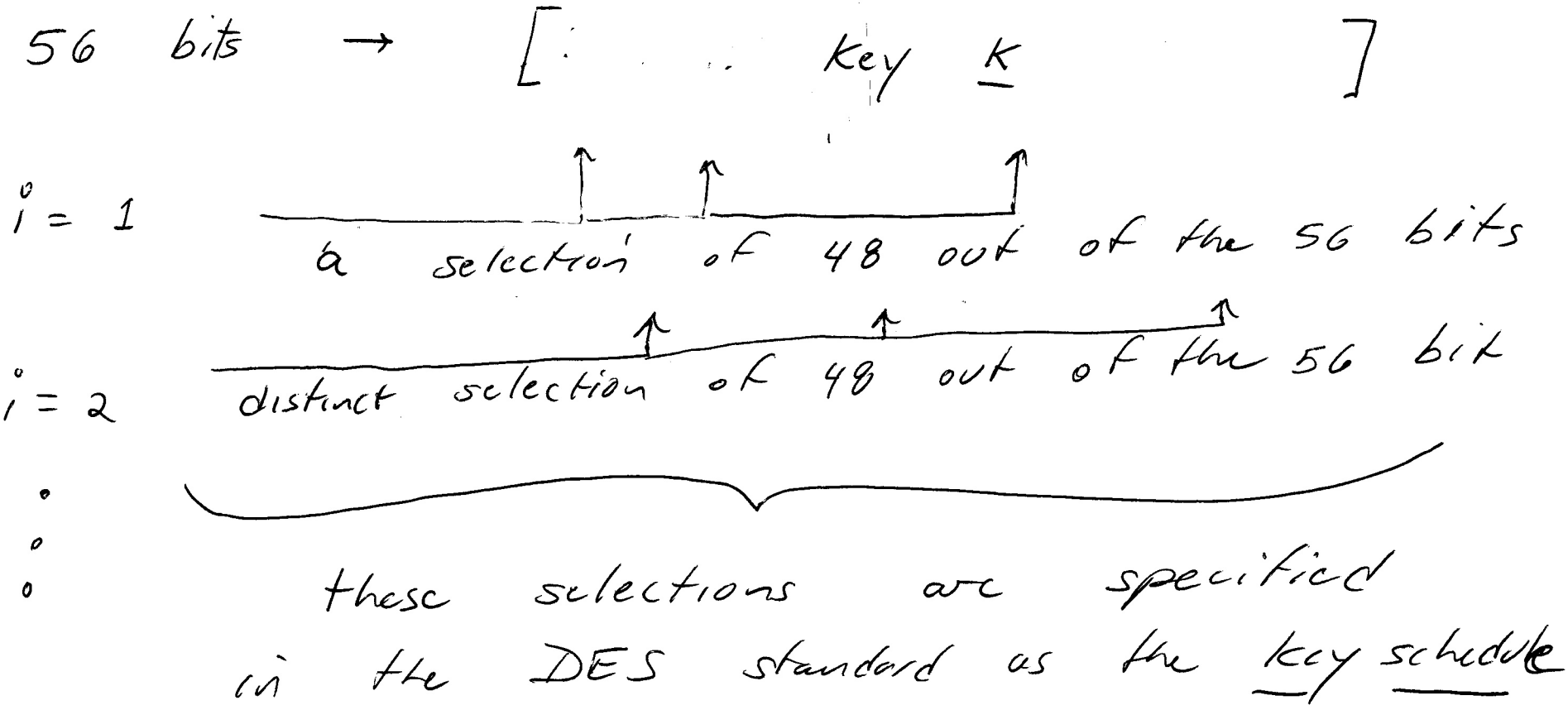
Spring Semester 2021

- Goals Today: Finish high level description of DES
- Observe that nonlinear encryption functions need not be closed under composition ⇒ multiple encryption steps become practically useful
- Structure of attacks on double encryption when attack has known plaintext / cipher-text
- Relation to "Birthday Problem": expected number of plaintext/ciphertext samples needed before attacker sees a repeated key

As noted in previous lecture (and Bach notes p. 27-1), high level view of DES; per 64-bit block:



• From the 56-bit "master" key, 16 × 48-bit subkeys are produced, K_i, $i = 1, 2, \ldots, 16$



Particular form of the b_{k_i} functions:

$$b_{k_i} : Z_2^{32} \to Z_2^{32}$$

so input is a 32-bit string.

Step 1: The 32-bit y input is expanded to 48-bit y^* (no new information: just repetition of certain bits in prescribed pattern): the DES expansion table

$$y^* = y[32], y[1], y[2], y[3], y[4], y[5], y[4], y[5] \ldots$$

see Bach p. 27-2 for more complete repetition specification.

So $y^* \in \mathbb{Z}_2^{48}$; (this 48-bit expansion matches subkey's length)

The 48-bits of $z = y^* + k_i$

into eight(8) 6-bit sub-blocks.

Each of these eight blocks is

operated on by an $S_k : \mathbb{Z}_2^6 \to \mathbb{Z}_2^4$

$k = 1, 2, \ldots 8$. In the terminology

of the DES standard, these

S_k functions are termed "S-boxes,"

and are specified by look-up tables.

As observed in Bach notes (p. 27-4),

S_k functions chosen to be strongly nonlinear.

The eight S_k functions together yield a result $\underline{w} \in \mathbb{Z}_2^{32}$

$$\underbrace{\underline{w}}_{\substack{32\text{-bit} \\ \text{result}}} = \begin{bmatrix} S_1(z_1) \\ S_2(z_2) \\ \vdots \\ S_8(z_8) \end{bmatrix} \quad \begin{matrix} \leftarrow 6\text{-bits} \\ \\ \\ \\ \end{matrix} \quad \begin{matrix} \} 4\text{-bits} \\ \} 4\text{-bits} \\ \\ \} 4\text{-bits} \end{matrix}$$

Then (finally)

$$b_{ki} = \underbrace{\pi\text{-permutation}}_{\substack{\text{a specific} \\ \text{permutation defined} \\ \text{in the DES standard}}} \text{ of } \underline{w}$$

Again: useful to be aware of the types of detail that go into constructing an encryption standard such as DES. But some of the details represent arbitrary or dated historical choices ⇒ don't worry too much about details for 435.

Key feature of interest, distinct from many prior encryption schemes examined in 435: the $e_k(x)$ defined by DES is <u>nonlinear</u>.

We motivated need for nonlinear $e_k(\cdot)$ from perspective that it would make computation of $d_k(\cdot)$ from known plaintext/ciphertext more difficult ("$e_k(\cdot)$ harder to invert").

Q: What other beneficial features are enabled by a nonlinear $e_k(\cdot)$?

Background Observation: For many of the previous classes of $e_k(\cdot)$ functions examined in 435, the function class was "closed under composition."

In simple terms, if we tried choosing $k_1 \neq k_2$, and building an encryption $e_{k_2}(e_{k_1}(x))$, there was always a k_3 such that $e_{k_3}(x) = e_{k_2}(e_{k_1}(x))$

Example: Hill ciphers.

Suppose we choose

$M_1, M_2 \in$ set of invertible matrices in $\mathbb{Z}_2^{m \times m}$,

construct an encryption

$$y = M_2 \cdot (M_1 \cdot x)$$

Have we created anything "new," beyond the class of Hill ciphers?

Obviously no, because

$M_3 = M_2 \cdot M_1 \in$ set of invertible matrices in $\mathbb{Z}_2^{m \times m}$

A set of 1-1, onto functions that is closed under composition is known as a "group".

Our classes of linear ciphers have all typically formed groups ⇒ no value in composing multiple applications of the same type of encryption function.

Answer to question "what new features are enabled by a class of nonlinear encryption functions?"

Much less likely to form a group.

In particular, DES encryption functions are not a group.

⇒ Multiple applications of DES (with distinct keys) can achieve "new" encryptions, not achievable by a single application of DES.

This motivates examination of cryptanalysis ("attacks") on double encryption.

Notation:

$$e_{k_1, k_2}(x) = e_{k_2}(e_{k_1}(x))$$

treat the two keys together as overall key

Still assume block structure, block size m, individual key length (for k_1, k_2) of ℓ. ($\overset{\text{all in}}{Z_2}$)

Again, treat attack strategy as an "intelligent" search for key values, k_1, k_2, with quality of strategy judged by reducing search to less than exhaustive case of $2^{(2\ell)}$.