Classical Ciphers (cont.)

Example: Viegenere Cipher - how to decipher ???

Assume the keyword size is known = n.

Ideally would know the number of characters in the keyword. Once the keyword is decrypted, the rest is easy …

Plaintext: HOW ARE YOU TODAY …

Key: ? ? ? ? ? ? ? ? ? ? ? ? ? ?

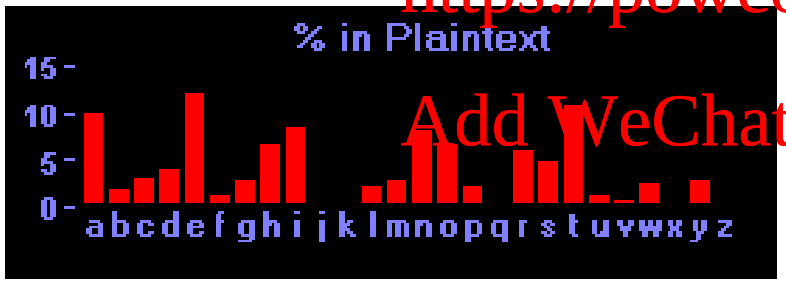
Ciphertext: TIQ ITC SCC VAXSG

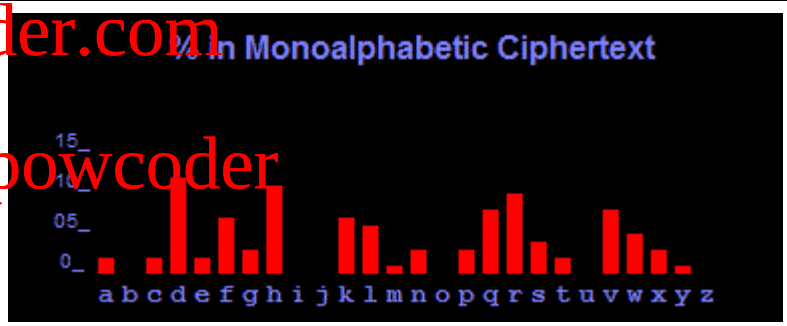
Total number of keys = 26^n.

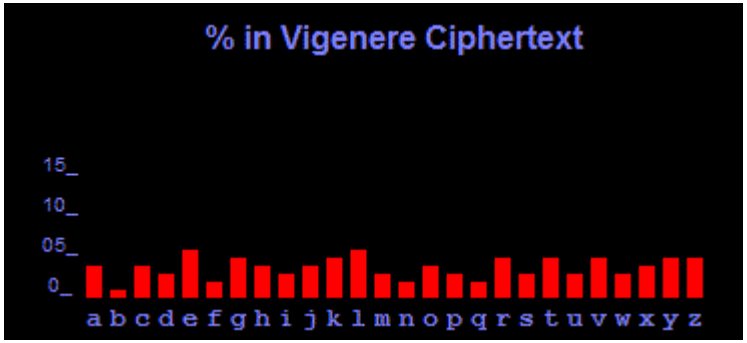
Classical Ciphers (cont.)

- Polyalphabetic / Vigenere Cipher (cont.)
  - Why is it so strong?

Aged twenty six, Vigènere was sent to Rome on a diplomatic mission. It was here that he became acquainted with the writings of Alberti, Trithemius and Porta, and his interest in cryptography was ignited. For many years, cryptography was nothing more than a tool that helped him his diplomatic work, but at the age of thirty-nine, Vigenère decided that he had amassed enough money to be able to abandon his career and concentrate on a life of study. It was only then that he began research into a new cipher.



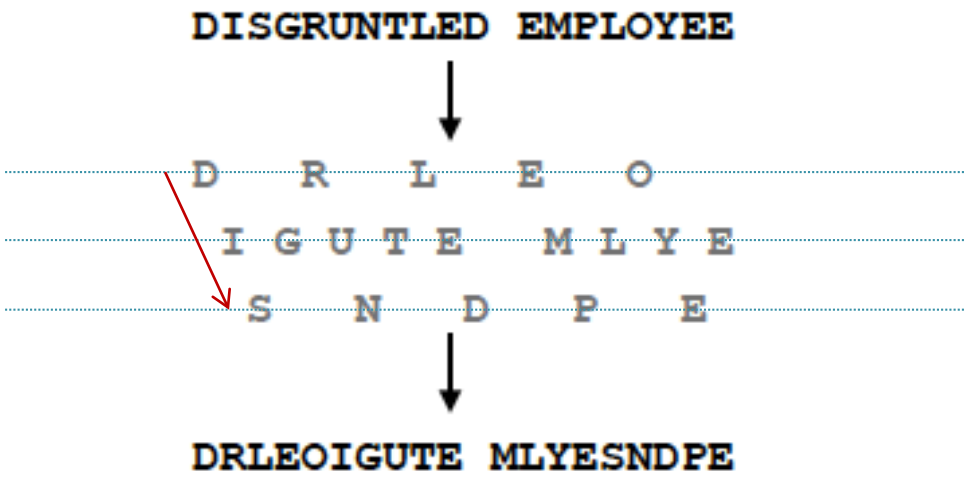




http://www.simonsingh.net/The_Black_Chamber/vigenere_strength.html

Classical Ciphers (cont.)

- **Transposition Cipher** – order of letters in the ciphertext is rearranged according to some predetermined method
- **Rail Fence Cipher** – transposition cipher in which the plaintext is written downwards and upwards on successive *'rails' of an imaginary fence*
  - the message is then read off in rows



Classical Ciphers (cont.)

Example: Rail Fence Cipher

Plaintext: DEFEND THE EAST WALL

2-Rail Fence Ciphertext: DFNTEATALEEDHESWL

D		F		N		T		E		A		T		A		L
	E		E		D		H		E		S		W		L	

3-Rail Fence Ciphertext: DNETLEEDHESWLFTAA

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Classical Ciphers (cont.)

Example: How to break a 2-rail cipher?

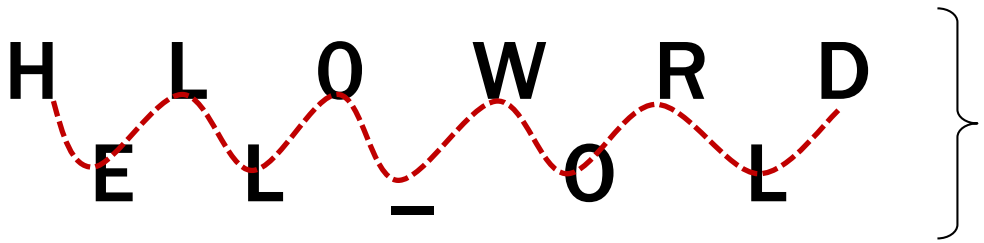
HLOWRDEL OL

Decrypting algorithm:

1) Count the letters in the cipher.
2) Divide the letters in 2 equal parts.

3) Draw/write the letters in a 2-rail zigzag pattern with ½ of the letters on the top and ½ of the bottom rail.

If number of letters is odd, add extra letter to the top rail.



HELLO WORLD

Classical Ciphers (cont.)

Example: How to break a 3-rail cipher?

M _ AETM _ T6EE _

Decrypting algorithm:

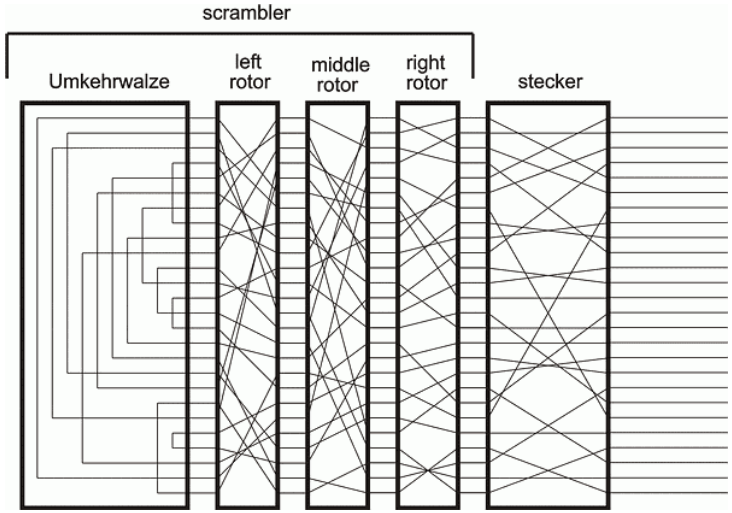
1) Count the number of letters.
2) Make an outline of the zigzag pattern with the given number of rails and given number of letters.

3) Arrange the letters at the allocated spaces …

M				_				A			
	E		T		M		_		T		6
		E				E				_	

Rotor Machines

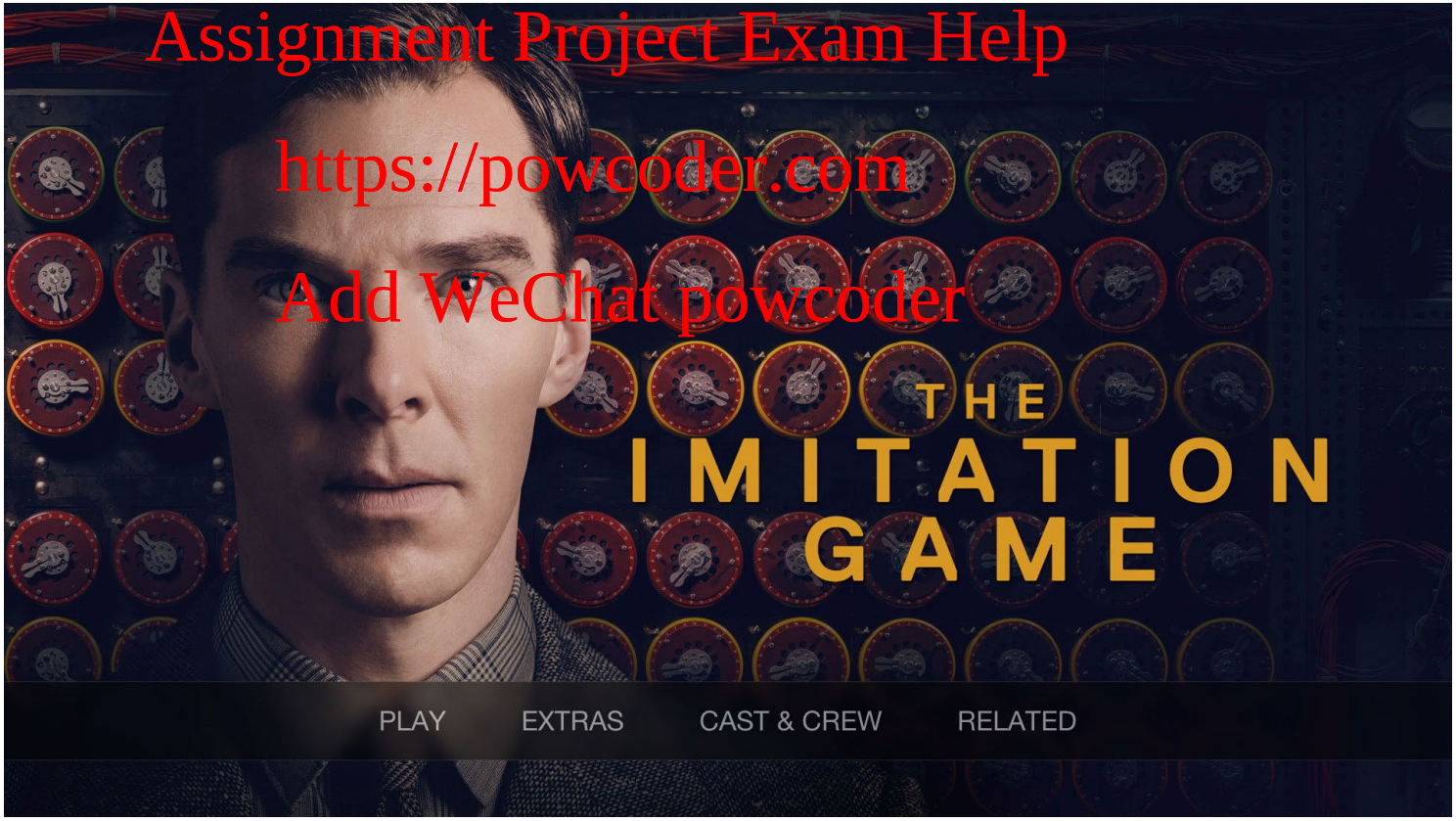
- **Rotor Machines** – mechanical devices for implementing complex substitution cipher
  - in widespread use 1920 – 1970 – most famous example is German Enigma machine from World War II
  - consists of keyboard (input letter), set of rotors, lights (output letter)
  - every time a key is pressed, some of the rotors change position, producing different output letter



https://www.advanced-ict.info/javascript/enigma.html

Rotor Machines (cont.)

http://www.telegraph.co.uk/culture/film/11229586/Imitation-Game-how-did-the-Enigma-machine-work.html



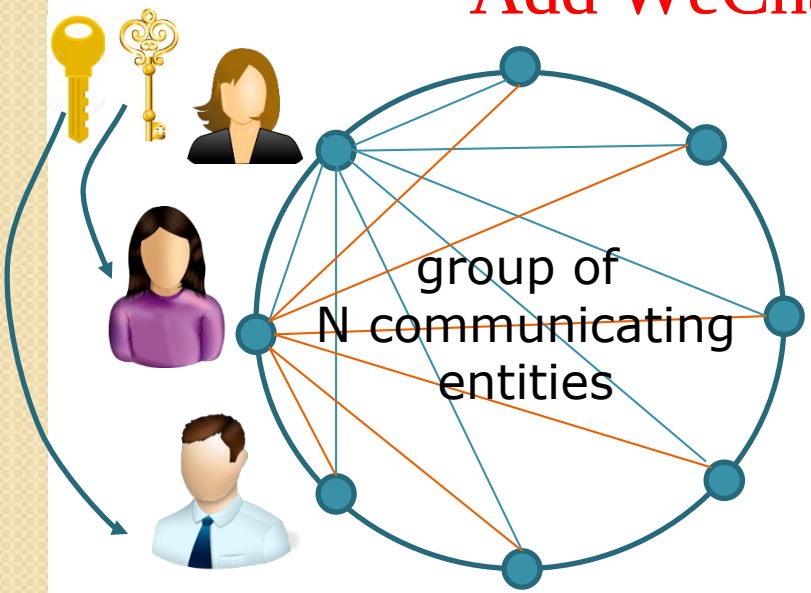
Modern Cryptography

Symmetric Encryption

Public Encryption

Symmetric Ciphers

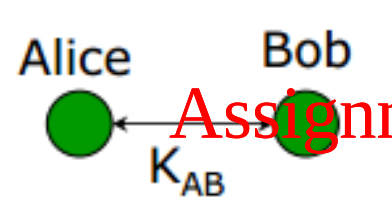
- **Symmetric Encryption** – private-key encryption - uses the same secret/private key to encrypt & decrypt information
  - symmetric key = shared secret – must only be known to the communicating parties – challenge # 1
  - to ensure full confidentiality in a group of N users, each pair of users must share a unique key – challenge # 2



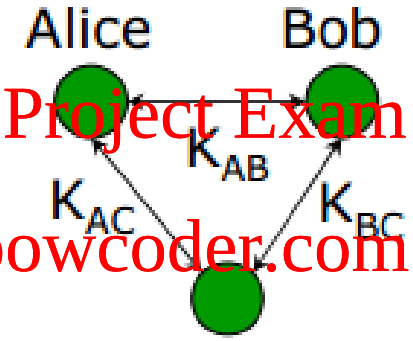
total number of keys required = (N-1)+(N-2)+(N-3)+...+1 = ((N-1)*N)/2

Symmetric Ciphers (cont.)

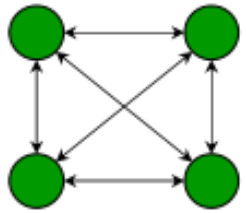
Example: Private-key encryption – number of keys



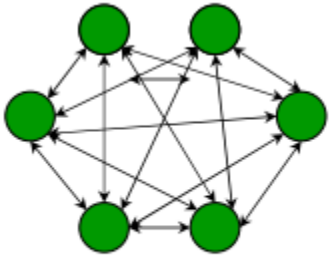
2 users: 1 key



3 users: 3 keys



4 users: 6 keys



6 users: 15 keys

100 users: 4950 keys

1000 users: 499,500 keys

Symmetric Ciphers (cont.)

Example: Symmetric Key Distribution

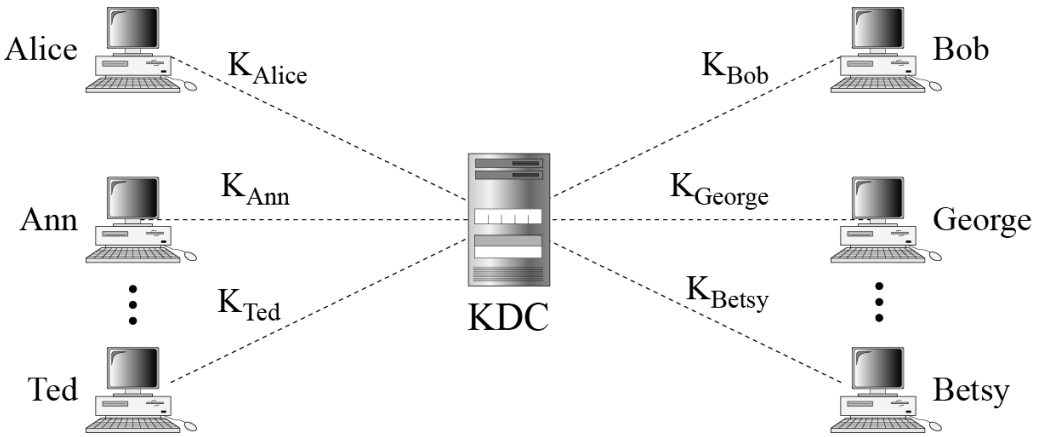
In systems deploying symmetric encryption both the number and distribution of keys is a problem.

Solution: Key Distribution Center (KDC) – trusted 3rd party/server.

Each entity shares a secret key with KDC - N keys in total.

KDC hands out keys to each pair of communicating entities (M) on demand, to enable confidential communication between them.

After use, keys are 'recycled'.

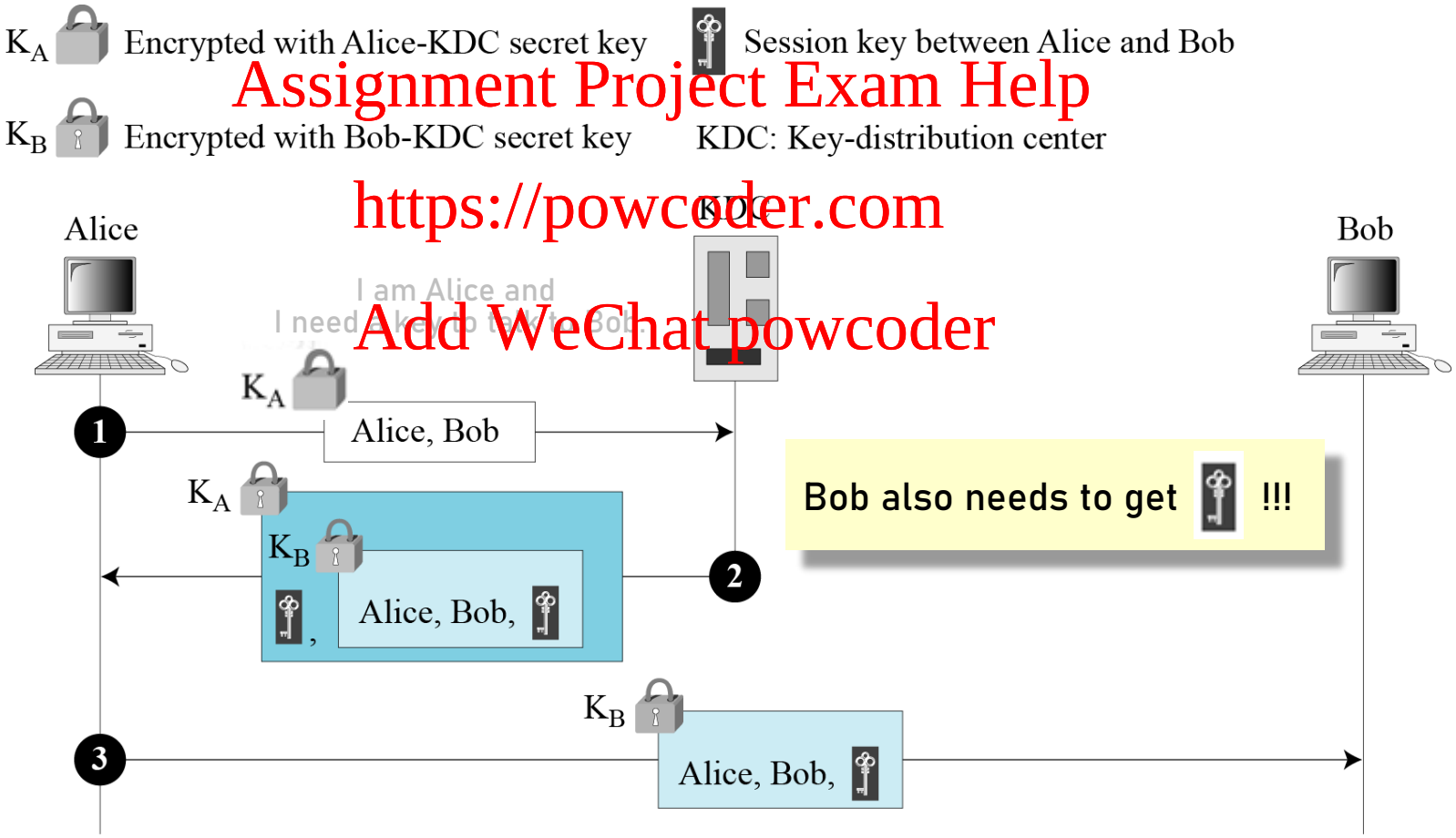


total number of keys in use in the system = = N + M

Symmetric Ciphers (cont.)

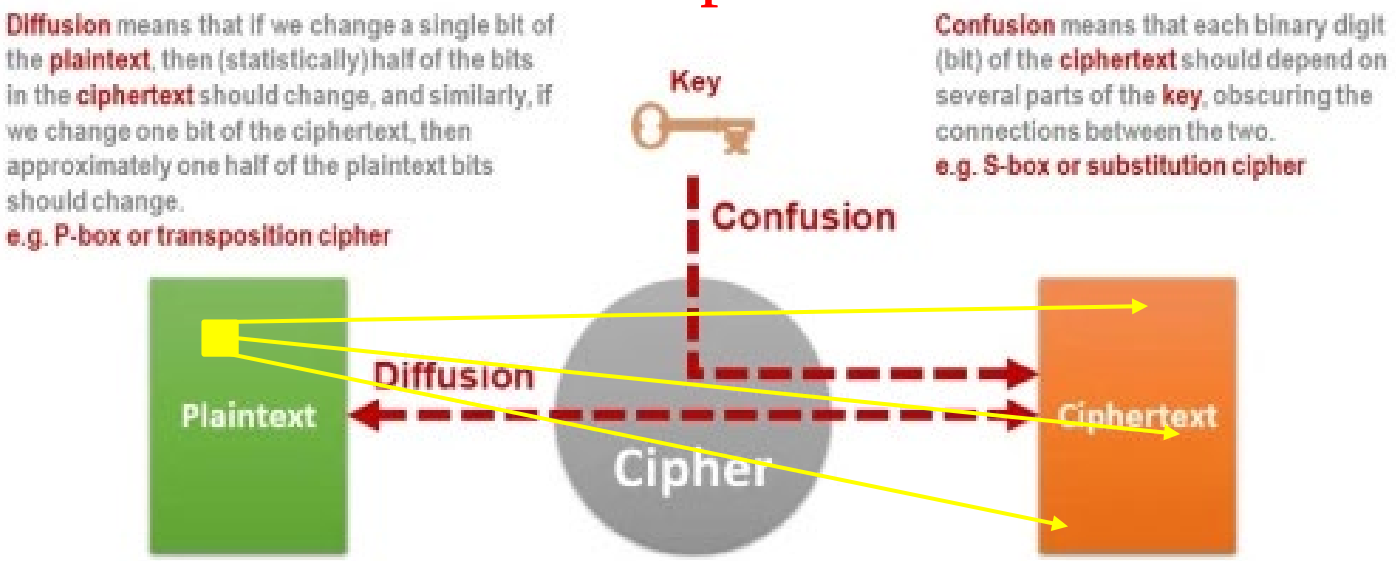
Example: Symmetric Key Distribution (cont.)

Possible solution.



Symmetric Ciphers (cont.)

- **Confusion vs. Diffusion** – desired crypto properties …
  - confusion = making the plaintext-ciphertext substitution (i.e., relationship between the key and the ciphertext) as complex and involved as possible
  - diffusion (permutation) = ensuring that the statistics of the plaintext is dissipated in the statistics of the ciphertext



Symmetric Ciphers (cont.)

- categories of Symmetric Encryption:

  a) **Stream Cipher** – encrypt digits (bytes) of a message one at a time

  → advantage: speed of transformation – each symbol is encrypted as soon as it is read

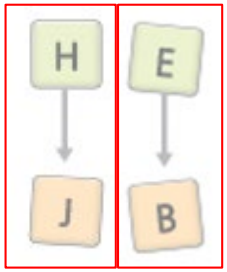
  → disadvantage: low diffusion – all information of a plain-text symbol is contained in a single ciphertext symbol

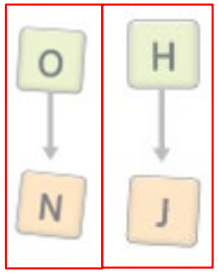
  → disadvantage: sensitivity to tampering – an interceptor can splice together pieces of previous messages and transmit a new message that looks authentic

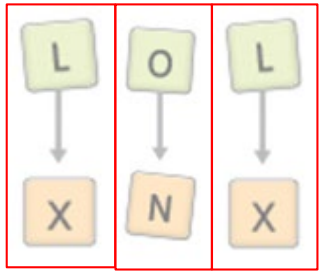
  → examples: **RC4**, **ChaCha**, **FISH, SEAL, …**

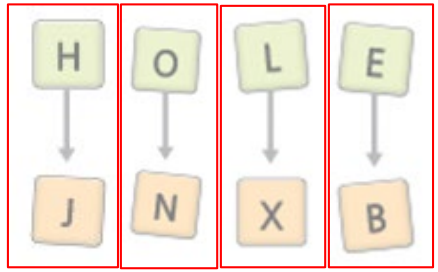
Symmetric Ciphers (cont.)

Example: simple message modification attack



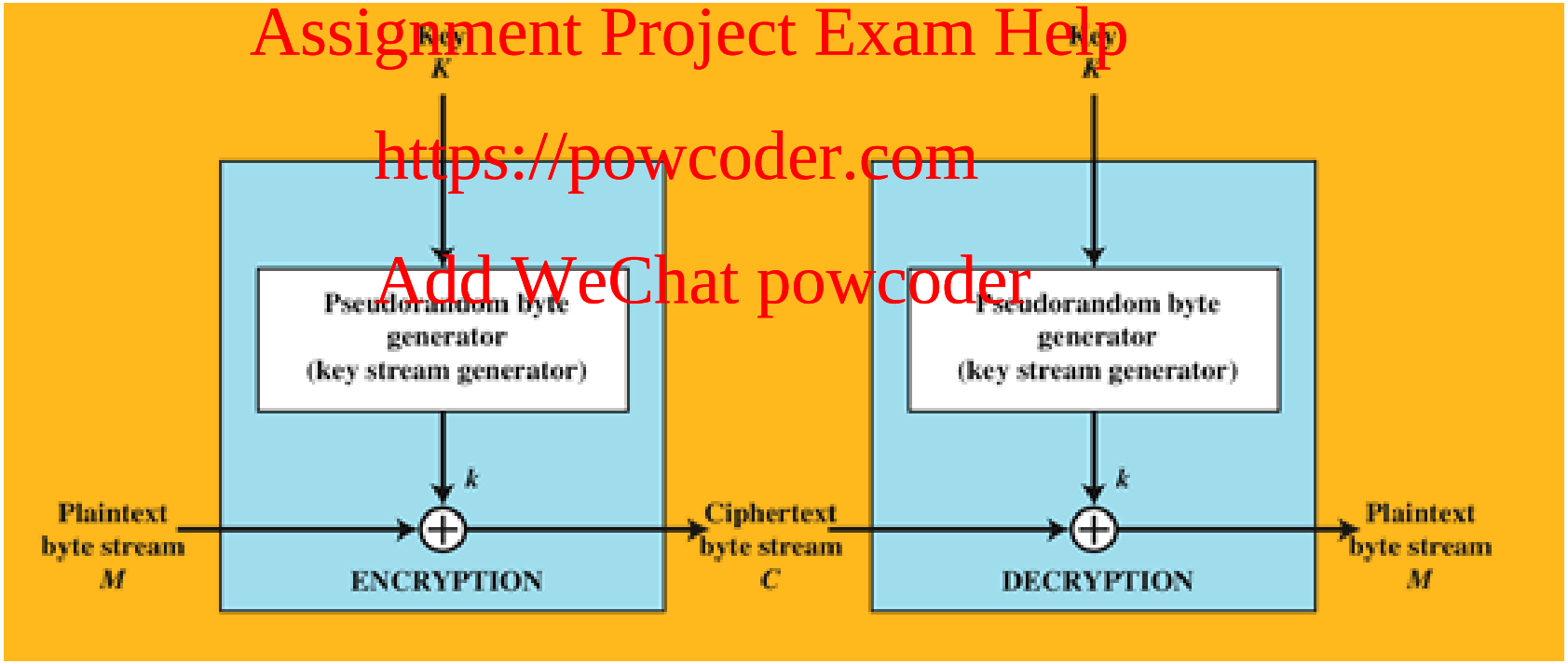






Symmetric Ciphers (cont.)

- categories of symmetric encryption:
  - a) **Stream Cipher** – improvement: pseudo-randomized key



key changes in pseudo-random manner – hard for attacker to predict, yet fully known to communicating parties

Symmetric Ciphers (cont.)

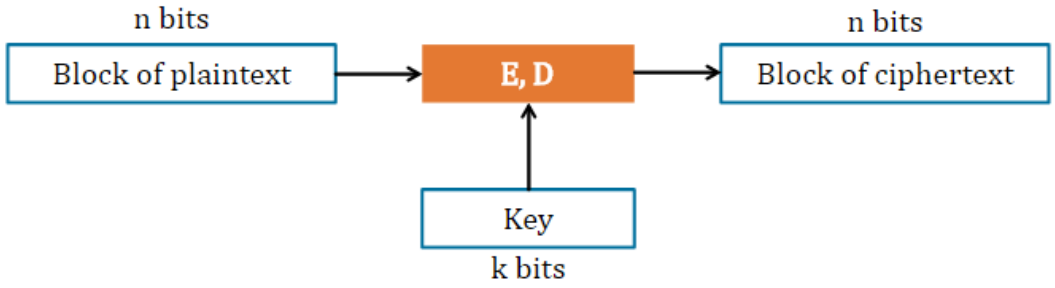
- categories of symmetric encryption (cont.)

b) **Block Cipher** – data is divided into fixed length blocks – all block bits are then acted upon to produce an output

→ advantage: high diffusion – information from one plaintext symbol is diffused into several ciphertext symbols

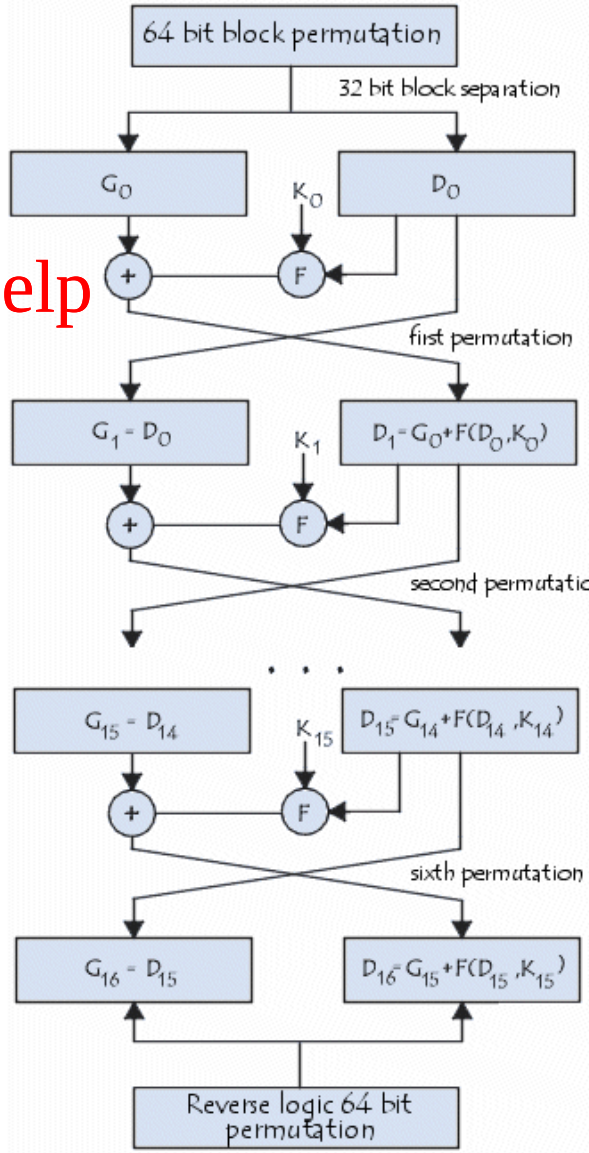
→ disadvantage: slowness of encryption – an entire block must be accumulated before encryption / decryption can begin => slows down real-time app.

→ examples: **DES**, **3DES**, **AES**



Symmetric Ciphers: DES

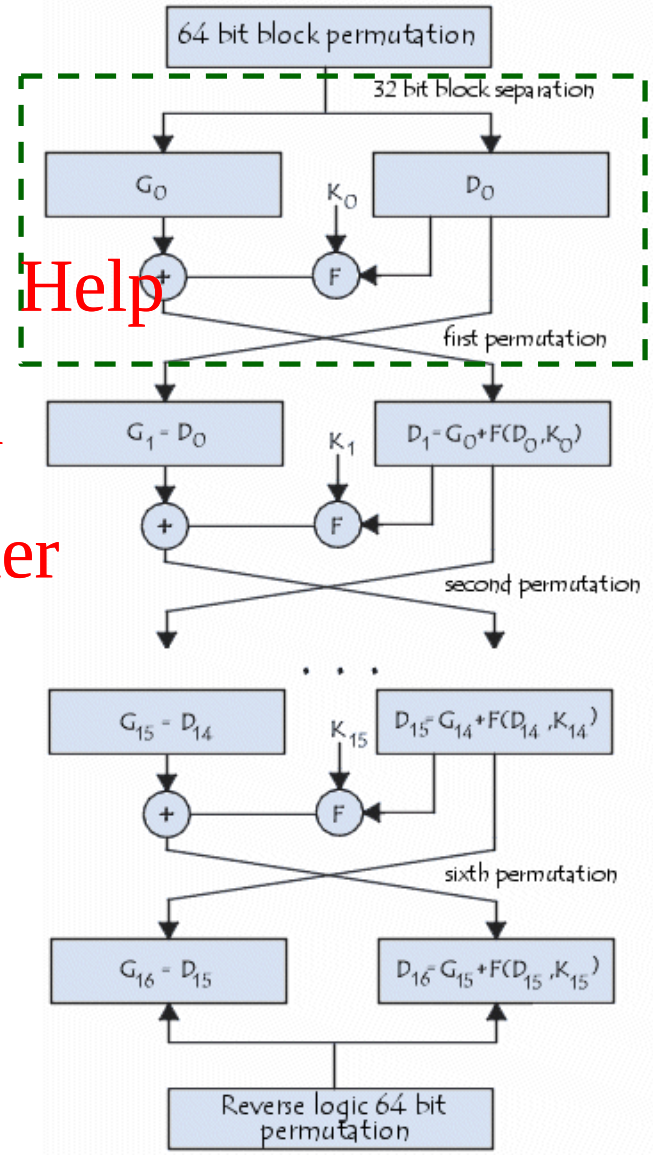
- **DES** – Data Encryption Standard
  - one of the first widely used symmetric-key block ciphers
  - *initially proposed by IBM (1974), later modified & adopted by US National Bureau of Standards (1977) as an official Federal Information Processing Standard (FIPS)*
  - takes a 64-bit block of plaintext and a 56-bit key to produce a ciphertext block of 64 bits
  - in 1999, Electronic Frontier Foundation managed to break DES in 22 h, 15 min
  - officially retired in 2005
  - 2-key variant of 3DES retired in 2015



Symmetric Ciphers: DES (cont.)

- DES – Data Encryption Standard
  - **algorithm:**

1) plaintext is fractioned into 64-bit blocks
2) each block is broken into two parts – left (L) and right (R)
3) permutation and substitution are repeated **16 times/rounds**
4) each round also uses a **48-bit subkey from the original 56-bit key**
5) in the end, two parts are re-joined and undergo inverse initial permutation



Symmetric Ciphers: DES (cont.)

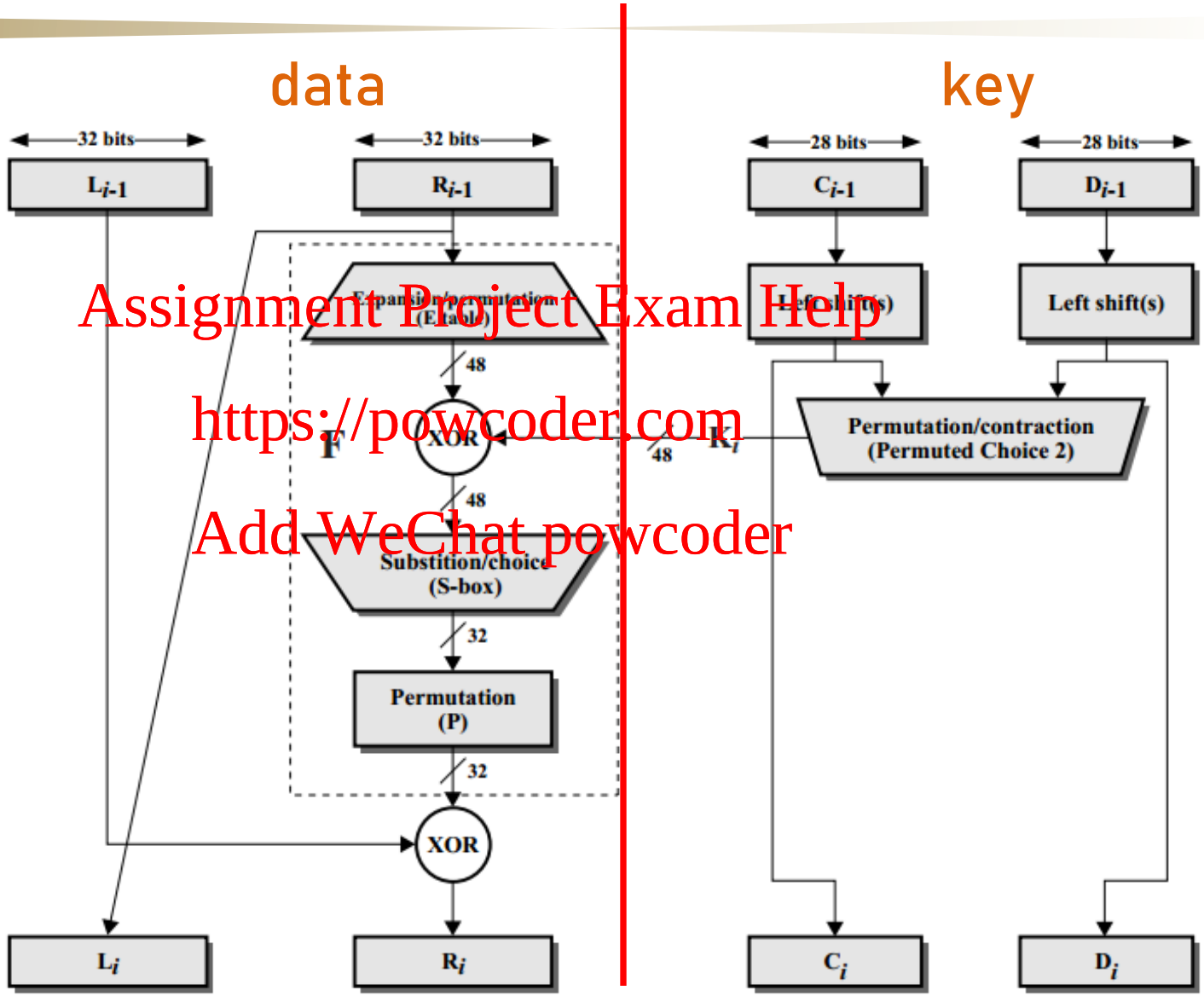
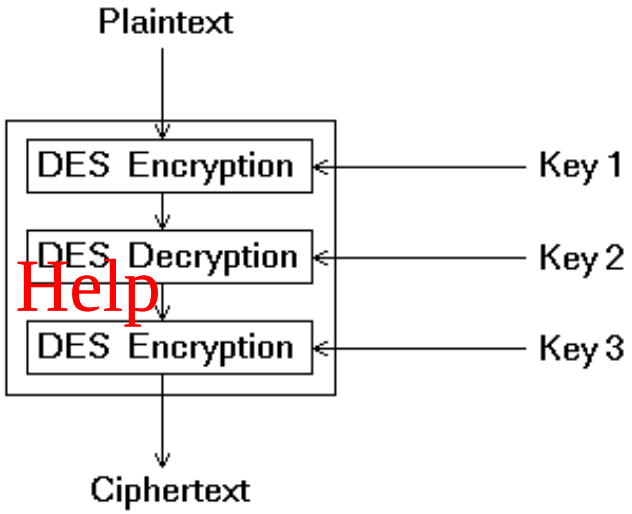


Figure 3.8 Single Round of DES Algorithm

Symmetric Ciphers: 3DES

- **Triple DES = TDES = 3DES**
  - symmetric-key block cipher which applies DES 3 times to each data block = Encrypt + Decrypt + Encrypt

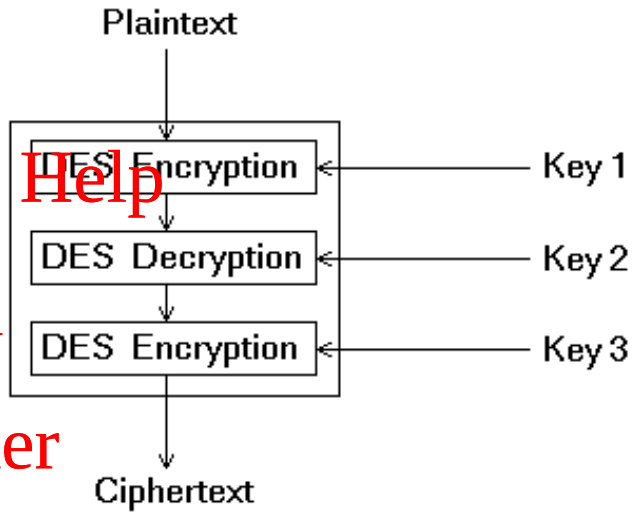


$$Ciphertext = E_{K3}(D_{K2}(E_{K1}(Plaintext)))$$

  - proposed in 1978, accepted as FIPS in 1999
  - a simple method of strengthening (increasing key size of) DES, without the need to design a completely new algorithm
  - current use – electronic payment industry

Symmetric Ciphers: 3DES (cont.)

- **Triple DES Keying Options**
  - Option 1: all three keys are independent
    - total key size = 168 bits
    - effective security = 112 bits
    - strongest
  - Option 2: K1 and K2 are independent, K3=K1
    - total key size = 112 bits
    - effective security = 80 bits
    - retired in 2015
  - Option 3: all three keys the same K1=K2=K3
    - total key size = 56 bits
    - weak – just a 'very slow' version of regular DES
    - no longer approved



Symmetric Ciphers: 3DES (cont.)

112-Bit Encryption With Two 56-Bit Keys

Sender	Receiver
Encrypts plaintext with the 1st key	Decrypts ciphertext with the 1st key
Decrypts output with the 2nd key	Encrypts output with the 2nd key
Encrypts output with the 1st key	Decrypts output with the 1st key

168-Bit Encryption with Three 56-Bit Keys

Sender	Receiver
Encrypts plaintext with the 1st key	Decrypts ciphertext with the 3d key
Decrypts output of first step with the 2nd key	Encrypts output of the first step with the 2nd key
Encrypts output of second step with the 3d key; gives the ciphertext to be sent	Decrypts output of second step with the 1st key; gives the original plaintext

Symmetric Ciphers: 3DES (cont.)

Triple DES – Pros and Cons

- 3DES, key option 1, still in use, but will be deprecated in 2023
  - many devices in the financial industry (e.g., POS terminals) as well as networking equipment (e.g., firewalls) use 3DES and are challenging to upgrade

- DES was designed for efficient hardware implementation - software implementation is very slow, 3DES even slower ☹
- DES and 3DES use 64-bit block size – to improve efficiency and security larger block sizes would be preferable ☹

overcome with AES