Test Your Tech

Crackers and cookies are:

A. Bytes to share with friends.

B. The best minor league baseball team of all time and their cheerleaders.

C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).

Test Your Tech

Crackers and cookies are:

A. Bytes to share with friends.

B. The best minor league baseball team of all time and their cheerleaders.

C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).

Announcements

- Due Dates
  - Today, 5pm
    - Lab 12
  - Monday, March 17, 11pm
    - Project 3B
    - Lab 14

Announcements

- Last week of class!
- No final exam!

Announcements

- Labs this week
  - Tuesday-Wednesday
    - Lab 14 on Security (required)
  - Thursday-Friday
    - Quiz on Chapter 17
    - TA evaluations
    - Project 3B work time
    - Pick up Reflection paper 3

Announcements

- Lecture this week
  - Today
    - Finish up SQL demonstrations
    - Security
  - Wednesday
    - Do computers think?
  - Friday
    - Reflection paper 4
    - Wrap-up
    - Course evaluations for lecture/instructor

Demonstrations (continued)

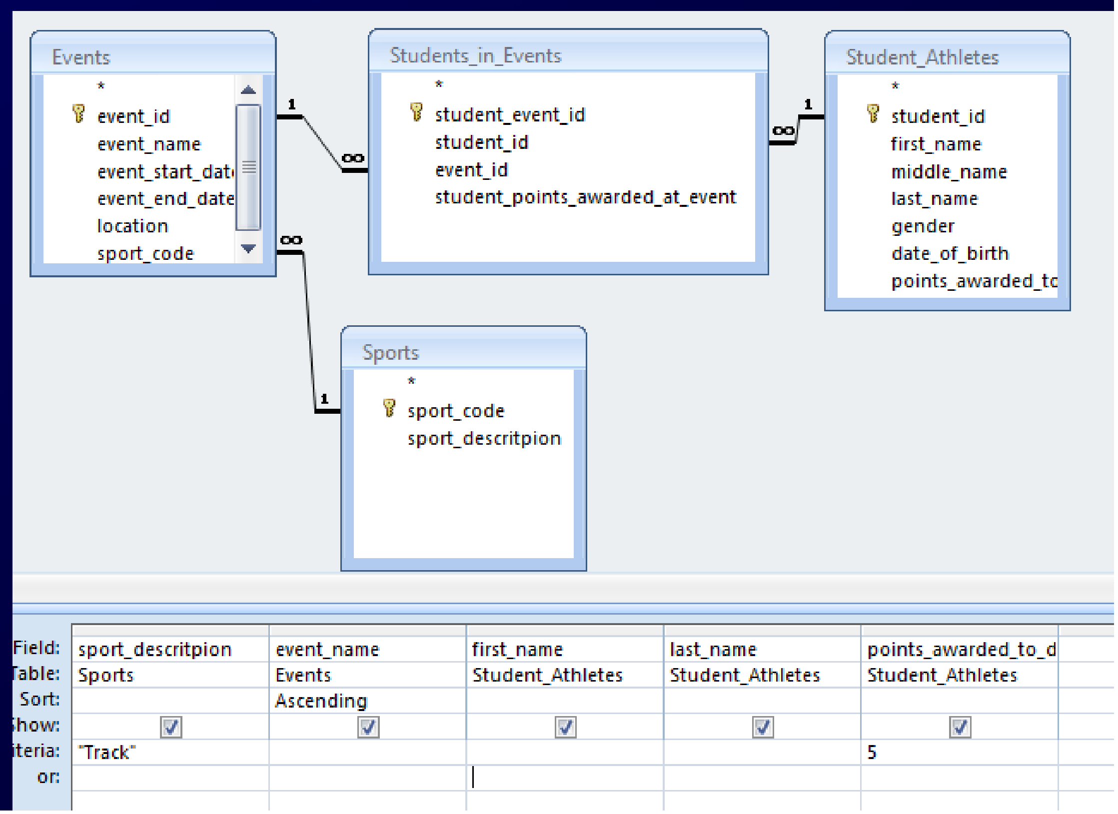
MORE SQL EXAMPLES

Queries

11. List all the events involving track and students who have earned at least 5 points.

Queries

11. List all the events involving track and students who have earned at least 5 points.

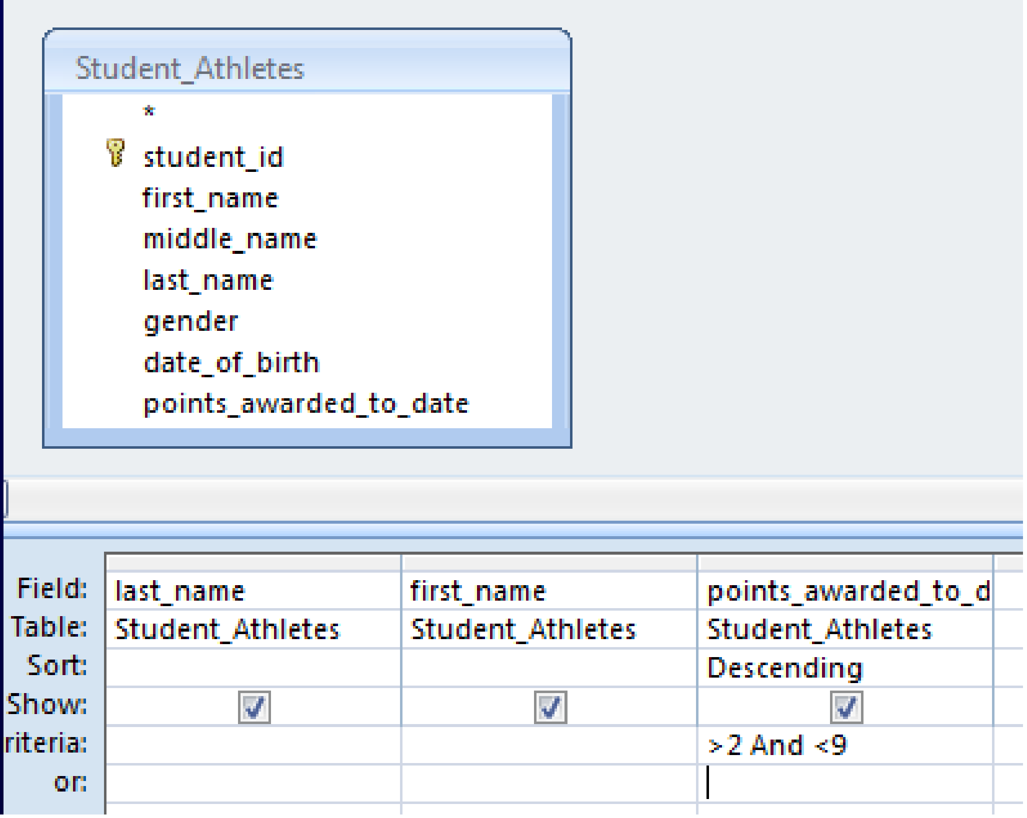


Queries

12. List all students who have earned between 2 and 9 points sorted with highest points first.

Queries

12. List all students who have earned between 2 and 9 points with highest points listed first.



Queries

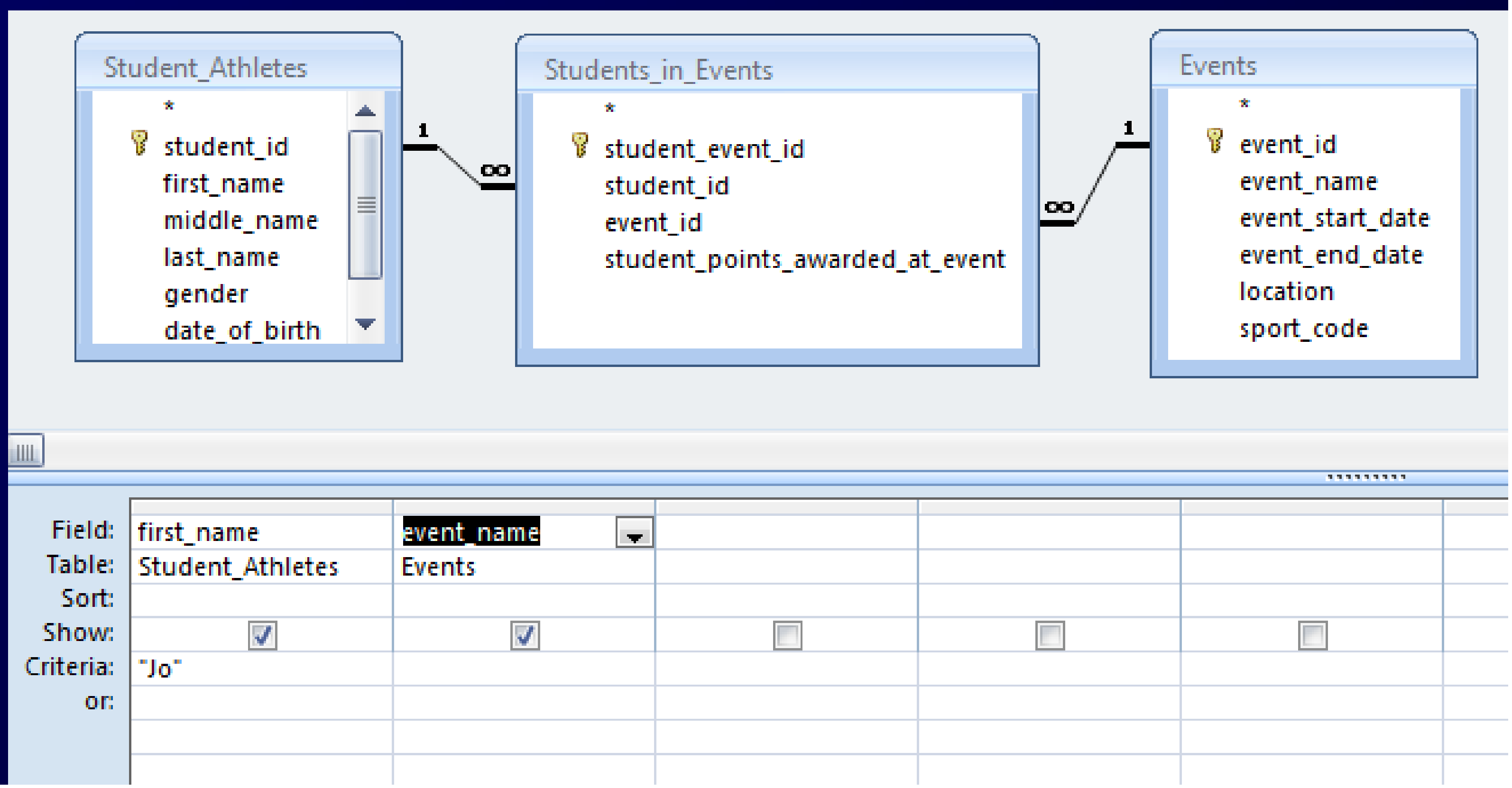
13. Show a listing of the average number of points won by students in each sport.

Queries

13. What events, if any, has Jo participated in?

Queries

13. What events, if any, has Jo participated in?

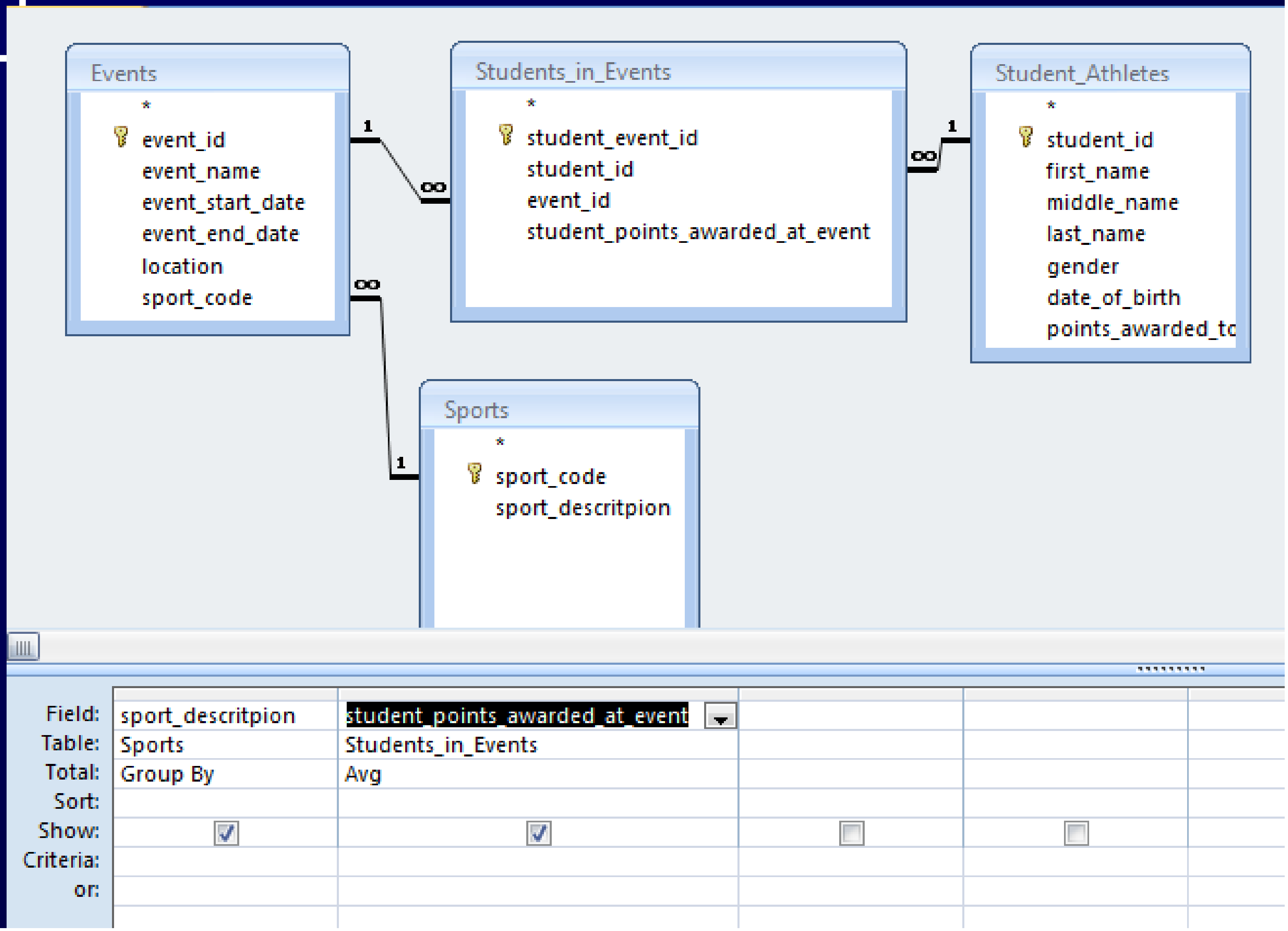


Queries

14. Show a listing of the average number of points won by students in each sport.

Queries

14.



Events
*
event_id
event_name
event_start_date
event_end_date
location
sport_code
Students_in_Events
*
student_event_id
student_id
event_id
student_points_awarded_at_event
Student_Athletes
*
student_id
first_name
middle_name
last_name
gender
date_of_birth
points_awarded_tc
Sports
*
sport_code
sport_descritpion
1
∞
Field: sport_descritpion | student_points_awarded_at_event
Table: Sports | Students_in_Events
Total: Group By | Avg
Sort:
Show:
Criteria:
or:

Queries

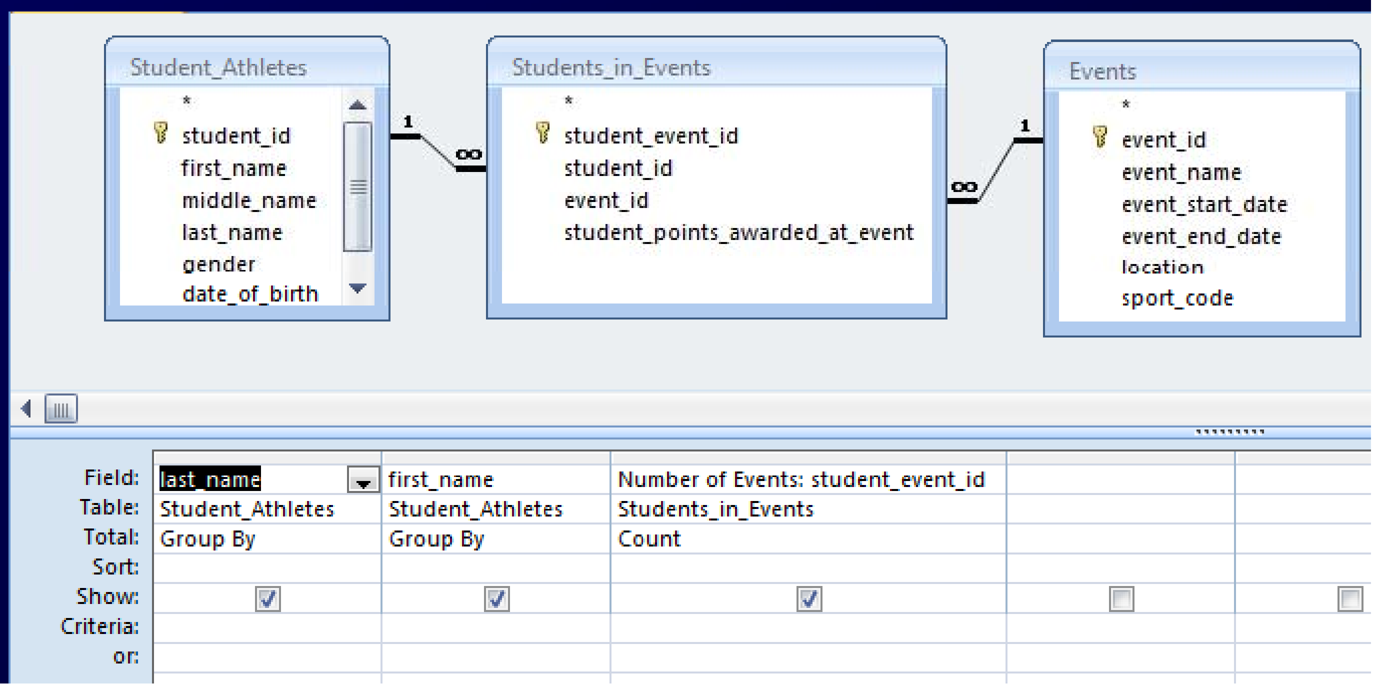
15. List the athletes' names and the number of events entered by each athlete but do not show the cases where only one event was entered.

Queries

15. a. Start by listing the athletes' names and the number of events entered by each athlete.

Queries

15. a. Start by listing the athletes' names and the number of events entered by each athlete.

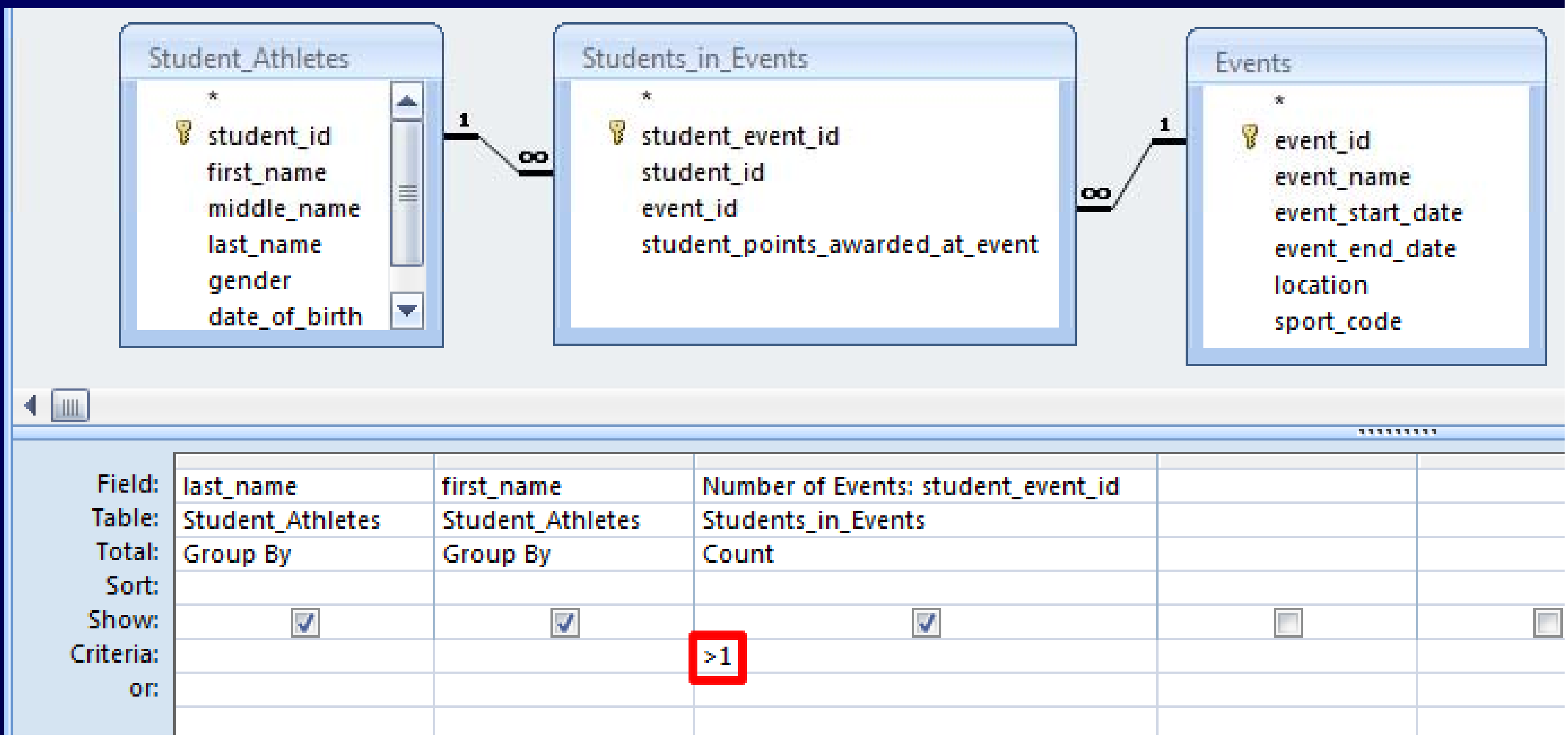


Queries

15. b. List the athletes' names and the number of events entered by each athlete but do not show the cases where only one event was entered.

Queries

15. b.



Student_Athletes
*
student_id
first_name
middle_name
last_name
gender
date_of_birth
Students_in_Events
*
student_event_id
student_id
event_id
student_points_awarded_at_event
Events
*
event_id
event_name
event_start_date
event_end_date
location
sport_code
1
∞
1
∞
Field: last_name | first_name | Number of Events: student_event_id
Table: Student_Athletes | Student_Athletes | Students_in_Events
Total: Group By | Group By | Count
Sort:
Show:
Criteria: >1
or:

Security

Video

- Encryption

Encryption And Decryption

- Encryption Terminology
  - *Encryption*: Transform representation so it is no longer understandable
  - *Cryptosystem*: A combination of encryption and decryption methods
  - *Cleartext* or *Plaintext*: Information before encryption
  - *Cipher text*: Information in encrypted form
  - *One-way cipher*: Encryption system that cannot be easily reversed (used for passwords)
  - *Decryption*: Reversing encryption process

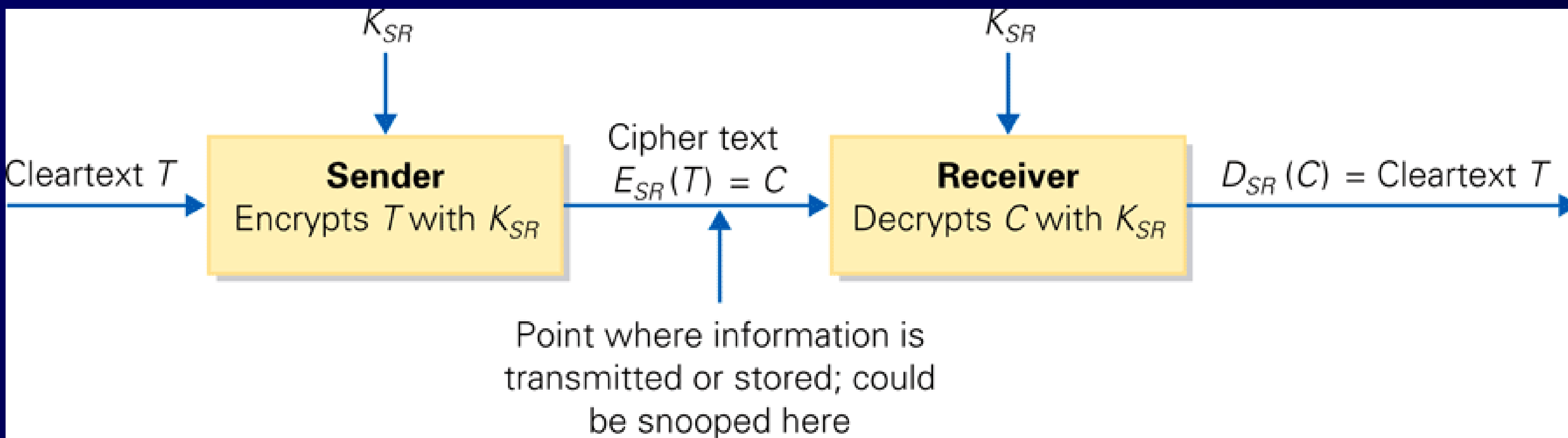


Figure 13.2 Schematic diagram of a cryptosystem. Using a key K_{SR} known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext.

XOR: An Encryption Operation

- Exclusive OR (XOR): Interesting way to apply a key to cleartext
- Combines two bits by rule: If the bits are the same, the result is 0; if the bits are different, the result is 1
- XOR is its own inverse (to decrypt back to original text)

Encrypting a Message

- Two students writing messages to each other decide to encrypt them
- Key is 0001 0111 0010 1101
- They use XOR encryption
- First write down ASCII representation of the letters in pairs
- XOR each resulting 16-bit sequence with their key
- If any bit sequence is XORed with another bit sequence and the result is XORed again with the same key, the result is the original bit sequence
- It makes no difference if the key is on the left or right

Cleartext		Key	Cipher Text	
Me	0100 1101 0110 0101		0101 1010 0100 1000	ZH
et	0110 0101 0111 0100		0111 0010 0101 1001	rY
@1	0100 0000 0011 0001		0101 0111 0001 1100	W^{F}_{S}
2:	0011 0010 0011 1010	⊕ 0001 0111 0010 1101 =	0010 0101 0001 0111	$\%^{E}_{\Sigma}$
15	0011 0001 0011 0101		0010 0110 0001 1000	$\&^{C}_{N}$
@J	0100 0000 0100 1010		0101 0111 0110 0111	Wg
oe	0110 1111 0110 0101		0111 1000 0100 1000	xH
's	0010 0111 0111 0010		0011 0000 0101 1111	0_

Figure 13.3 Encrypting the cleartext `Meet@12:15@Joe's`, using ASCII encoding of letter pairs, the key `0001 0111 0010 1101`, and the operation of exclusive OR to produce the cipher text ZHrY$W^{F}_{S}\%^{E}_{\Sigma}\&^{C}_{N}$WgxH0_. (Decryption works in the opposite direction, as if the "⊕" and "=" symbols of the figure were exchanged.)

Breaking the Code

- Longer text is easier to decode
  - Notice what bit sequences show up frequently
  - Knowledge of most frequent letters in the cleartext language
    - e is the most common letter in English
- Smarter byte-for-byte substitutions
  - Group more than two bytes
  - Be sure not to exchange the key over unsecured connection

Public Key Cryptosystems

- People who want to receive information securely publish a key that senders should use to encrypt messages
- Key is chosen so only receiver can decode

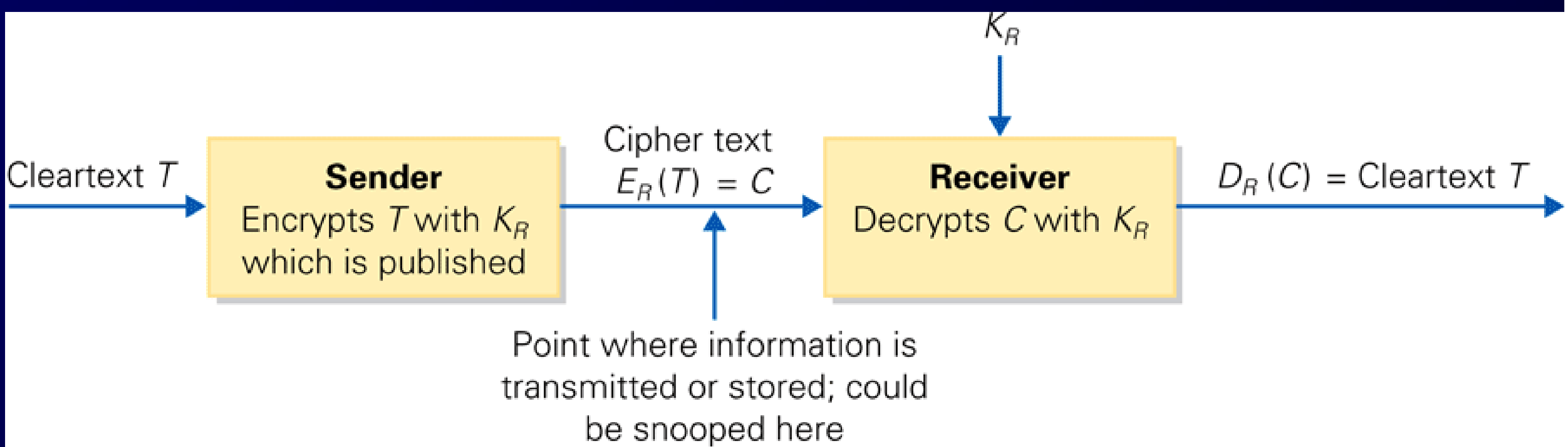


Figure 13.4 Public key cryptosystem. The sender uses the receiver's public key K_R to encrypt the cleartext, and only the receiver is able to decrypt it to recover the cleartext.

Code Cracker's Problem

- How is it secure when the key is published?
- All that is sent is the remainder
  - Bits left over from dividing manipulated data by the key
- So how can the receiver decrypt?

RSA
Public Key Cryptosystem

- Relies on prime numbers
- Any number can be factored into primes in only one way
- Choosing a Key:
  - ∗ Key has special properties
    - Must be the product of two different prime numbers, *p* and *q*
      - – $K_R = pq$
    - *p* and *q* must be about 64 or 65 digits long to produce a 129-digit public key
    - *p* and *q* must also be 2 greater than a multiple of 3

Encrypting a Message

- Divide cleartext into blocks, cube the blocks, divide them by the public key, and transmit the remainders from the divisions

The Decryption Method

- Compute the quantity $s = (1/3)(2(p-1)(q-1) + 1)$
- If the cipher text numbers C are each raised to the s power, C^s, and divided by the key K_R, the remainders are the cleartext
- That is for some quotient c that we don't care about:
  - $C^s = K_R * c + T$

Summarizing the RSA System

- Three steps:
  - Publishing
  - Encrypting
  - Decrypting
- As long as *p*, *q*, and *s* are kept secret, code can't be cracked
  - If the key is large enough, factoring to find p and q can't be done in any reasonable amount of time even by software

Strong Encryption Techniques

- A communicating party can use the technology to protect their communication so no one else can read it, period
- Government agencies would like this technology kept out of the hands of "bad guys"
- What if cryptography software vendors had to give government a way to break such codes?

Strong Encryption Techniques

- Trapdoor Technique:
  - Way to bypass security while software is encrypting the cleartext. Send cleartext to law-enforcement officials when cipher text is sent.
- Key escrow:
  - Require software to register key with a third party, who holds it in confidence. If there is a need to break the code, the third party provides the key.
- These two schemes could be abused

Redundancy Is Very, Very, Very Good

- Precautions against data disasters include backups and system redundancy (having a hot spare up and running)

A Fault Recovery Program for Business or You!

- Keep a full copy of everything written on the system as of some date and time—full backup
- Create partial backups—copies of changes since last full backup
- After disaster, start by installing the last full backup copy
- Re-create state of system by making changes stored in partial backups, in order
- All data since last backup (full or partial) will be lost

Backing Up a Personal Computer

- How and What to Back Up
  - ∗ You can buy automatic backup software that writes to zip drive or writeable CD
  - ∗ For manual backups, you do not have to backup data that
    - Can be re-created from some permanent source, like software
    - Was saved before but has not changed
    - You don’t care about

Recovering Deleted Information

- Backups also protect from accidental deletions
- Can save evidence of crime or other inappropriate behavior
- Remember that two copies of email are produced when sender hits send—one in sent mail file and one somewhere else, which the sender probably can't delete