CHAPTER 13

- **Asymmetric encryption algorithm:** An encryption algorithm in which the key for encryption and the key for decryption are different, with the encryption key being public and the decryption key being secret; also called a public key encryption algorithm.
- **Attribute:** A category of information in a tuple.
- **Authentication:** The process of verifying the identity of the receiver of a message.
- **B2B (business-to-business) Web site:** A Web site whose purpose is to streamline transactions between a company as the seller and other businesses as buyers.
- **B2C (business-to-consumer) Web site:** A Web site whose purpose is to advertise a company's products and to allow online purchasing by the general public.
- **Banner ad:** A graphical ad, often with animation, placed in a prominent position on a Web page.
- **Bit:** The most basic unit of data; a value of 0 or 1.
- **Byte:** A group of eight bits.
- **Ciphertext:** A message that is encrypted.
- **Cookie:** A small text file that the Web server sends to the user's browser and that gets stored on the user's hard drive.
- **Data file:** A file containing related records.
- **Database management system (DBMS):** A system that manages the files in a database.
- **Database:** A collection of related data files.
- **Domain name:** A company's homepage URL.
- **E-business:** A concept in which orders are processed, credit is verified, transactions are completed, debits are issued, shipping is alerted, and inventory is reduced, all electronically.
- **E-commerce:** A concept in which financial transactions are conducted by electronic means.
- **Encryption:** The process of encoding the data to be transmitted into a scrambled form using a scheme agreed upon between the sender and the receiver.
- **Field:** A group of bytes used to represent a string of characters.
- **In-house development:** The development of a company's e-commerce Web site by the employees of the company.
- **Middleware:** Software that allows separate, existing programs to communicate and work together seamlessly.
- **Outsourcing:** Giving a particular project over to another company.
- **Plaintext:** A message that is not encrypted.
- **Portal:** An entry point Web page with links to other Web pages on some topic.
- **Primary key:** An attribute or combination of attributes that uniquely identifies a tuple.
- **Public key encryption algorithm:** An encryption algorithm in which the key for encryption and the key for decryption are different, with the encryption key being public and the decryption key being secret; also called an asymmetric encryption algorithm.
- **Record:** A collection of related fields.

- **Relational database model:** A model of a database in which a data file is conceptually represented as a two-dimensional table.
- **SSL (secure sockets layer):** A series of protocols that allow a client (the Web browser) and a Web server to agree on the encryption methods to be used, exchange the necessary security keys, and authenticate the identity of each party to the other.
- **Stream cipher:** An encryption algorithm that encodes one character at a time.
- **Substitution cipher:** An encryption algorithm in which a single letter of plaintext generates a single letter of ciphertext.
- **Symmetric encryption algorithm:** An encryption algorithm in which a single secret key is used to both encrypt and decrypt the message.
- **Tuple:** A row of a table in a relational database model.