ষষ্ঠ অধ্যায় পাঠ-১০: ডেটাবেজ সিকিউরিটি।

এই পাঠ শেষে যা যা শিখতে পারবে-

১। ডেটাবেজ সিকিউরিটি ব্যাখ্যা করতে পারবে।

২। ডেটা এনক্রিপশন এর বিভিন্ন পদ্ধতি ব্যাখ্যা করতে পারবে।

ডেটাবেজ সিকিউরিটিঃ একটি ডেটাবেজে অনির্দিষ্ট ব্যবহারকারী থেকে ডেটা সুরক্ষিত রাখাকে বলা হয় ডেটাবেজ সিকিউরিটি।

ডেটাবেজ সিকিউরিটি নিচের বিষয়গুলোকে নিয়ন্ত্রণ করে:

১। ব্যবহারকারীর ডেটা ব্যবহার করার অধিকার সংরক্ষণ করা।

২। সিস্টেম রিসোর্স ব্যবহার নিয়ন্ত্রণ করা।

৩। ডিস্ক ব্যবহার নিয়ন্ত্রণ করা।

৪। ব্যবহারকারীর অ্যাকশন নিয়ন্ত্রণ করা।

৫। ব্যবহারকারীর ডেটা ব্যবহারের সীমা নির্ধারণ করা।

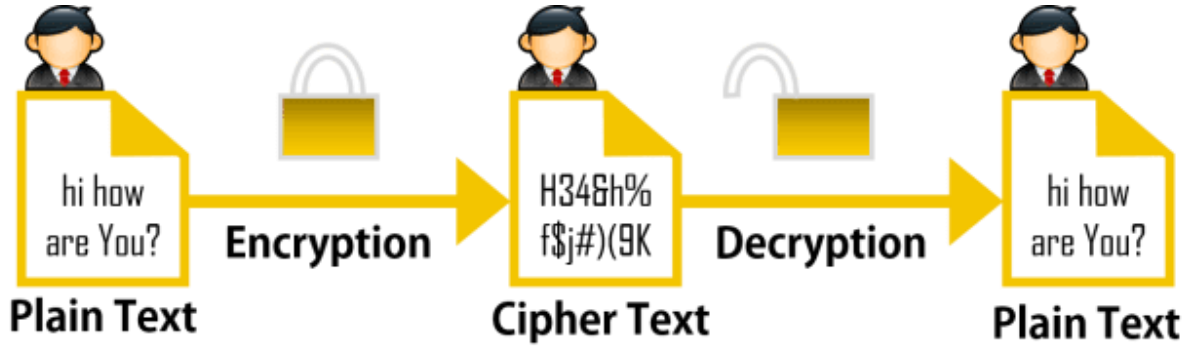
ডেটাবেজের সিকিউরিটি প্রধানত ২ ভাগে ভাগ করা যায়:

- ক। সিস্টেম সিকিউরিটি
- খ। ডেটা সিকিউরিটি

সিস্টেম সিকিউরিটি: ডেটাবেজের সিস্টেম লেভেলে অনির্দিষ্ট ব্যক্তির প্রবেশ রক্ষা করার জন্য গৃহীত ব্যবস্থাকে বলা হয় সিস্টেম সিকিউরিটি। সার্ভার কম্পিউটার অচল হয়ে গেলে ডেটাবেজের ডেটা হারিয়ে যায়। কিন্তু সিস্টেম সিকিউরিটি থাকলে ডেটা পুনরুদ্ধার করা যায়।

ডেটা সিকিউরিটিঃ অনির্দিষ্ট ব্যক্তির হাত থেকে ডেটার গোপনীয়তা রক্ষা করাকে বলা হয় ডেটা সিকিউরিটি। ডেটা সিকিউরিটির জন্য প্রাপককে ডেটা এনক্রিপ্ট করে পাঠানো হয়। প্রাপকের কাছে ডেটা পৌছানোর পর প্রাপক ডেটাকে ডেক্রিপ্ট করে তারপর ব্যবহার করে। ডেটাকে এনক্রিপশন ও ডিক্রিপ্টশন করার বিষয়কে ক্রিপ্টোগ্রাফী বলে।

ডেটা এনক্রিপশন এবং ডিক্রিপ্টশনঃ যে প্রক্রিয়ায় প্লেইনটেক্সটকে পরিবর্তন করে ছাইফারটেক্সট তৈরি করা হয় তাকে এনক্রিপশন বলে। যে প্রক্রিয়ায় ছাইফারটেক্সটকে পরিবর্তন করে পুনরায় প্লেইনটেক্সট তৈরি করা হয় তাকে ডিক্রিপ্টশন বলে।উৎস ডেটাকে এনক্রিপ্ট করে পাঠালে প্রাপককে ঐ ডেটা ব্যবহারের পূর্বে ডিক্রিপ্ট করতে হয়। প্রেরক এবং প্রাপককে যথাক্রমে এনক্রিপ্ট এবং ডিক্রিপ্ট করার পদ্ধতি/ অ্যালগরিদম জানতে হয়।



ডেটা এনক্রিপশনের প্রধান চারটি অংশঃ

- ১। প্লেইনটেক্সট (Plain Text)
- ২। সাইফারটেক্সট (Cipher-text)
- ৩। এনক্রিপশন অ্যালগরিদম (Encryption Algorithm)
- ৪। সিকিউরিটি কী বা কোড (Security key or Code)

প্লেইনটেক্সট (Plain Text): এনক্রিপ্ট করার পূর্বের ডেটা যা পাঠ করা যায় তাকে প্লেইনটেক্সট বলে।

সাইফারটেক্সট (Cipher-text): এনক্রিপ্ট করার পরের ডেটা যা পাঠ করা যায় না তাকে সাইফারটেক্সট বলে।

এনক্রিপশন অ্যালগরিদম (Encryption Algorithm): যে গাণিতিক ফর্মুলার মাধ্যমে প্লেইনটেক্সট থেকে সাইফারটেক্সট আবার সাইফারটেক্সট থেকে প্লেইনটেক্সট এ রুপান্তর করা হয় তাকে এনক্রিপশন অ্যালগরিদম বলে।

সিকিউরিটি কী বা কোড (Security key or Code): যে গোপন সংকেত বা কোডের মাধ্যমে ডেটা এনক্রিপ্ট ও ডিক্রিপ্ট করা হয় তাকে সিকিউরিটি কী বা কোড।

ডেটা এনক্রিপ্ট করার বিভিন্ন পদ্ধতিঃ

- ১। সিজার কোড (Caesar Code)
  ২। ডেটা এনক্রিপশন স্ট্যান্ডার্ড (Data Encryption Standard-DES)
  ৩। ইন্টারন্যাশনাল ডেটা এনক্রিপশন অ্যালগরিদম (International Data Encryption Algorithm-IDEA)

এনক্রিপশন পদ্ধতি-১:

এ পদ্ধতিতে ইংরেজি প্রত্যেক বর্ণের জন্য নির্দিষ্ট ক্রম অনুযায়ী নির্দিষ্ট বর্ণ ব্যবহার করা হয়। যেমন- ইংরেজি প্রত্যেক বর্ণকে তার পরবর্তী বর্ণ দ্বারা প্রতিস্থাপন করলে- ICT শব্দটির এনক্রিপশন হলো JDU । এখানে মূল শব্দের প্রত্যেক বর্ণের পরবর্তী বর্ণ ব্যবহার করে এনক্রিপ্ট করা হয়েছে।

এনক্রিপশন পদ্ধতি-২:

১। এ পদ্ধতিতে মূল ডেটার প্রত্যেক বর্ণকে ইংরেজি বর্ণমালার ক্রম অনুসারে অবস্থান নির্ণয় করা হয়। যেমন- A এর অবস্থানগত মান 1 এবং C এর অবস্থানগত মান 3।

২। অবস্থানগত সংখ্যাকে ৮ দ্বারা গুণ করা হয়।

৩। গুণফলের মানকে অবস্থান ধরে বর্ণমালার ক্রমানুসারে যে বর্ণটি পাওয়া যায় তা এনক্রিপ্টেড বর্ণ হিসাবে ধরা হয়।

৪। গুণফল ২৬ অপেক্ষা বড় হলে গুণফলকে ২৬ দ্বারা ভাগ করে ভাগশেষ নির্ণয় করা হয়। এক্ষেত্রে ভাগশেষের মানকে অবস্থান ধরে বর্ণমালার ক্রমানুসারে যে বর্ণটি পাওয়া যায় তা এনক্রিপ্টেড বর্ণ হিসাবে ধরা হয়।

এ পদ্ধতিতে CAESAR শব্দটি এনক্রিপ্ট করি-

C = 3 X8 = 24 → X
A = 1X8 = 8 → H
E = 5X8 = 40 → 40÷ 26 → ভাগশেষ 14 → N
S = 19X8 = 152 → 152÷26 → ভাগশেষ 22 → V
A = 1X8 = 8 → H
R = 18X8 = 144 → 144÷26 → ভাগশেষ 14 → N

সুতরাং **CAESAR** শব্দটি এনক্রিপ্ট হয়ে **XHNVHN** হয়ে গেল, যা **Cipher-text** হিসেবে পরিচিত।

পাঠ মূল্যায়ন-

জ্ঞানমূলক প্রশ্নসমূহঃ

- ক। ডেটা সিকিউরিটি কী?
- ক। ডেটা এনক্রিপশন কী?
- ক। ডেটা ডিক্রিপশন কী?

অনুধাবনমূলক প্রশ্নসমূহঃ

- খ। ডেটা সুরক্ষার পদ্ধতি ব্যাখ্যা কর।
- খ। ডেটা এনক্রিপশন করতে হয় কেন? ব্যাখ্যা কর।
- খ। প্লেইন টেক্সট ও সাইফার টেক্সট এক নয়- ব্যাখ্যা কর।
- খ। ডেটাবেজ নিরাপত্তায় এনক্রিপশন জরুরি কেন?
- খ। ব্যক্তিগত পর্যায়ে ডেটা সিকিউরিটি কীভাবে নিশ্চিত করা যায়?

সৃজনশীল প্রশ্নসমূহঃ

বহুনির্বাচনি প্রশ্নসমূহঃ

১। নিচের কোনটি ডেটা এনক্রিপশনের অংশ নয়?

ক) প্লেইন টেক্সট খ) সাইফার টেক্সট গ) এলগরিদম ঘ) প্যারিটি বিট

২। ডেটা এনক্রিপশন সংশ্লিষ্ট বিষয় হলো-

i. প্লেইনটেক্সট ii. সাইফার টেক্সট iii. কী

নিচের কোনটি সঠিক?

ক) i ও ii খ) i ও iii গ) ii ও iii ঘ) i, ii ও iii

৩। ডেটার গোপনীয়তা রক্ষায় গৃহীত ব্যবস্থা কোনটি?

ক) এনক্রিপশন খ) প্লেইন টেক্সট গ) সর্টিং ঘ) ইন্ডেক্সিং

৪। ডেটা এনক্রিপ্টশন ও ডিক্রিপ্টশনের নিয়ম কোনটি?

ক) সাইবারনেট্রিক্স খ) ক্রিপ্টোগ্রাফী গ) ইনফরমেট্রিক ঘ) সাইটোগ্রাফি

৫। ডেটা এনক্রিপশনের প্রয়োজন হয়-

ক) ডেটা ম্যানেজমেন্টে খ) ডেটা সর্টিং-এ গ) ডেটা সিকিউরিটিতে ঘ) ডেটা পরিবর্তনে