অধ্যায়-৪ ডাটা সিকিউরিটি

SOS অতি সংক্ষিপ্ত প্রশ্নোত্তর ঃ

*** ১। ডাটাবেস সিকিউরিটি কাকে বলে?**

উত্তর ঃ ডাটাবেসে জমা রাখা তথ্য যেন কেউ চুরি করতে না পারে, ভুলভাবে পরিবর্তন করতে না পারে এবং প্রয়োজনে যেন সবসময় পাওয়া যায়–তা নিশ্চিত করাই হলো ডাটাবেস সিকিউরিটি।

***** ২। DES ও AES কী?** বাকাশিবো- ২০২৫

উত্তর ঃ DES ঃ Data Encryption Standard(DES) হলো একটি ঐতিহাসিক এবং গুরুত্বপূর্ণ এনক্রিপশন পদ্ধতি, যা ডিজিটাল তথ্যকে সুরক্ষিত করতে ব্যবহৃত হতো। এটি একটি Symmetric-key অ্যালগরিদম, অর্থাৎ এখানে তথ্য এনক্রিপ্ট এবং ডিক্রিপ্ট করার জন্য একই Key ব্যবহার করা হয়।

AES ঃ Advanced Encryption Standard (AES) হলো বর্তমানে বিশ্বের সবচেয়ে জনপ্রিয় এবং শক্তিশালী এনক্রিপশন অ্যালগরিদম।

এটি ইলেকট্রনিক ডাটা বা তথ্যকে কোড এ রূপান্তর করে সুরক্ষিত রাখে।

**** ৩। হ্যাশিং অ্যালগরিদম (Hashing Algorithm) কী?**

উত্তর ঃ হ্যাশিং অ্যালগরিদম হলো একটি গাণিতিক ফাংশন যা যেকোনো দৈর্ঘ্যের ডাটা গ্রহণ করে সেটিকে একটি নির্দিষ্ট দৈর্ঘ্যের অনন্য ডিজিটাল কোডে রূপান্তর করে। এই আউটপুটকে বলা হয় 'হ্যাশ ভ্যালু' বা 'মেসেজ ডাইজেস্ট'।

***** ৪। এন্ড-টু-এন্ড এনক্রিপশন কী?** বাকাশিবো-২০২৫

উত্তর ঃ এন্ড-টু-এন্ড এনক্রিপশন হলো ডেটা বা তথ্য সুরক্ষার এমন একটি পদ্ধতি, যেখানে শুধুমাত্র প্রেরক (Sender) এবং প্রাপক (Receiver) তথ্যটি পড়তে পারেন। মাঝপথে অন্য কেউ, এমনকি যে কোম্পানি বা সার্ভারের মাধ্যমে মেসেজটি যাচ্ছে, তারাও সেই তথ্য পড়তে পারে না।

**** ৫। ডিজিটাল সার্টিফিকেট (Digital Certificate) বলতে কী বুঝায়?**

উত্তর ঃ ডিজিটাল সার্টিফিকেট হলো ইন্টারনেটে কোনো ব্যক্তি, ওয়েবসাইট বা ডিভাইসের পরিচয় নিশ্চিত করার একটি ইলেকট্রনিক দলিল।

এটি অনেকটা আমাদের বাস্তব জীবনের পাসপোর্ট বা জাতীয় পরিচয়পত্রের মতো কাজ করে।

SOS সংক্ষিপ্ত প্রশ্নোত্তর ঃ

**** ১। ডাটা সিকিউরিটি এবং ডাটা প্রাইভেসির মধ্যে পার্থক্য লেখ।**

বিষয়	ডেটা সিকিউরিটি	ডেটা প্রাইভেসি
১.মূল সংজ্ঞা	এটি মূলত তথ্যকে অননুমোদিত প্রবেশ বা সাইবার আক্রমণ থেকে রক্ষা করার প্রক্রিয়া।	এটি মূলত তথ্যের সঠিক ব্যবহার, সংগ্রহ এবং আইনি অধিকার নিশ্চিত করার বিষয়।
২.প্রধান লক্ষ্য	ডেটা যাতে চুরি না হয় বা হ্যাক না হয় তা নিশ্চিত করা।	ডেটা কার সাথে শেয়ার করা হবে এবং ব্যবহারকারী তার তথ্যের ওপর কতটা নিয়ন্ত্রণ পাবেন তা নিশ্চিত করা।
৩. প্রযুক্তিগত দিক	এটি মূলত টেকনিক্যাল ব্যবস্থার ওপর নির্ভরশীল (যেমন: ফায়ারওয়াল, এনক্রিপশন)।	এটি মূলত আইনি এবং নীতিমালার ওপর নির্ভরশীল (যেমন: এউচজ বা গোপনীয়তা নীতি)।
৪.দায়বদ্ধতা	এটি নিশ্চিত করে যে ডেটা "সুরক্ষিত" আছে কি না।	এটি নিশ্চিত করে যে ডেটা "সঠিকভাবে এবং আইন মেনে" ব্যবহার হচ্ছে কি না।

***** ২। ক্রিপ্টোগ্রাফি ব্যাখ্যা কর।** বাকাশিবো- ২০২৫

উত্তর ঃ ক্রিপ্টোগ্রাফি (Cryptography) হলো তথ্যকে একটি গোপন কোডে রূপান্তর করার পদ্ধতি বা শিল্প, যাতে কেবল নির্দিষ্ট ব্যক্তিই সেই তথ্যটি পড়তে বা বুঝতে পারে। এটি মূলত তথ্যের গোপনীয়তা এবং সুরক্ষা নিশ্চিত করার জন্য ব্যবহৃত হয়।

ক্রিপ্টোগ্রাফি মূলত দুই ধরনের Key ব্যবহারের ওপর ভিত্তি করে ভাগ করা হয় ঃ

১) সিমেট্রিক ক্রিপ্টোগ্রাফি (Symmetric Cryptography) ঃ এখানে তথ্য এনক্রিপ্ট এবং ডিক্রিপ্ট–উভয় কাজের জন্যই একটি মাত্র কবু ব্যবহার করা হয়। এটি দ্রুত কাজ করে কিন্তু কবু টি সুরক্ষিতভাবে আদান-প্রদান করা কঠিন।

উদাহরণ ঃ AES, DES.

২) অ্যাসিমেট্রিক ক্রিপ্টোগ্রাফি (Asymmetric Cryptography) ঃ এখানে দুটি আলাদা কবু ব্যবহার করা হয়–একটি 'পাবলিক কী' এবং একটি 'প্রাইভেট কী' । এটি অনেক বেশি নিরাপদ।

উদাহরণ ঃ RSA, ECC.

***** ৩। এনক্রিপ্টেড ডাটা স্টোরেজের সুবিধাসমূহ লেখ।** বাকাশিবো- ২০২৫

উত্তর ঃ এনক্রিপ্টেড ডাটা স্টোরেজের সুবিধাসমূহ নিম্নরূপ ঃ

১. ডেটা চুরির ঝুঁকি হ্রাস (Protection Against Data Theft) ঃ যদি কোনো ল্যাপটপ, পেনড্রাইভ বা সার্ভার হার্ডডিস্ক চুরি হয়ে যায়, তবুও

হ্যাকার বা চোর সেই তথ্য দেখতে পারবে না। কারণ এনক্রিপশন করা ফাইলগুলো তাদের কাছে হিজিবিজি কোড হিসেবে থাকবে।

২. গোপনীয়তা রক্ষা (Enhanced Privacy) ঃ ব্যক্তিগত ছবি, ভিডিও বা প্রতিষ্ঠানের গোপন নথিপত্র অন্য কেউ (এমনকি স্টোরেজ প্রোভাইডার বা আইটি অ্যাডমিনও) দেখতে পারে না। এটি তথ্যের সর্বোচ্চ গোপনীয়তা নিশ্চিত করে।

৩. আইনি বাধ্যবাধকতা পূরণ (Compliance) ঃ অনেক আন্তর্জাতিক আইন (যেমনঃ GDPR বা HIPAA) অনুযায়ী গ্রাহকের তথ্য এনক্রিপ্ট করে রাখা বাধ্যতামূলক। এনক্রিপশন ব্যবহার করলে প্রতিষ্ঠানগুলো বিভিন্ন আইনি ঝামেলা ও জরিমানা থেকে মুক্তি পায়।

৪. ডাটার অখণ্ডতা বজায় রাখা (Data Integrity) ঃ এনক্রিপশন শুধুমাত্র তথ্য লুকায় না, এটি তথ্য পরিবর্তনের চেষ্টাও শনাক্ত করতে পারে। যদি কেউ এনক্রিপ্ট করা ফাইলে কোনো পরিবর্তন করার চেষ্টা করে, তবে ডিক্রিপশন করার সময় তা ধরা পড়বে এবং ফাইলটি ওপেন হবে না।

৫. ক্লাউড স্টোরেজে নিরাপত্তা (Cloud Security) ঃ গুগল ড্রাইভ বা ড্রপবক্সের মতো ক্লাউড সার্ভারে ডাটা রাখার সময় যদি তা এনক্রিপ্ট করা থাকে, তবে ক্লাউড সার্ভিস প্রোভাইডার হ্যাক হলেও আপনার ডাটা নিরাপদ থাকবে।

SOS রচনামূলক প্রশ্নোত্তর ঃ

**** ১। বিভিন্ন ধরনের ডাটা হাইডিং পদ্ধতি আলোচনা কর।**

উত্তর ঃ তথ্য গোপন রাখা বা ডাটা হাইডিং (Data Hiding) হলো এমন একটি কৌশল যার মাধ্যমে গোপন তথ্যকে এমনভাবে লুকিয়ে রাখা হয় যাতে অননুমোদিত কেউ এর অস্তিত্বই টের না পায়। সাইবার নিরাপত্তা এবং গোপন যোগাযোগের ক্ষেত্রে এটি অত্যন্ত গুরুত্বপূর্ণ।

নিচে বিভিন্ন ধরনের ডাটা হাইডিং পদ্ধতি সহজ ভাষায় আলোচনা করা হলো ঃ

১. স্টেনোগ্রাফি (Steganography) ঃ এটি ডাটা হাইডিংয়ের সবচেয়ে জনপ্রিয় পদ্ধতি। এতে গোপন তথ্যকে অন্য কোনো সাধারণ ফাইলের (যেমন- ছবি, অডিও বা ভিডিও) ভেতরে এমনভাবে লুকিয়ে রাখা হয় যে বাইরে থেকে দেখলে কিছুই বোঝা যায় না।

i) Image Steganography ঃ ছবির পিক্সেলের ভেতরে টেক্সট বা অন্য ফাইল লুকিয়ে রাখা।

ii) Audio/Video Steganography ঃ অডিও বা ভিডিও ফাইলের অপ্রয়োজনীয় ডাটা স্তরে তথ্য গোপন করা।

২. ক্রিপ্টোগ্রাফি (Cryptography) ঃ অনেকে একে আলাদা মনে করলেও এটি ডাটা হাইডিংয়ের একটি অন্যতম রূপ। এখানে তথ্যের অস্তিত্ব লুকানো হয় না, বরং তথ্যের অর্থ লুকিয়ে ফেলা হয়। সাধারণ টেক্সটকে এমন হিজিবিজি কোডে রূপান্তর করা হয় যা চাবি (Key) ছাড়া পড়া অসম্ভব।

৩. ফাইল মাস্কিং বা রিনেমিং (File Masking) ঃ এটি একটি সহজ পদ্ধতি যেখানে ফাইলের ধরন বা এক্সটেনশন বদলে দেওয়া হয়।

উদাহরণঃ একটি গুরুত্বপূর্ণ .zip ফাইলকে .txt বা .jpg নামে সেভ করে রাখা। এতে সাধারণ কেউ ফাইলটি খুললে শুধু ভুল কোড দেখতে পাবে।

৪. অল্টারনেট ডাটা স্ট্রিম (Alternate Data Streams - ADS) ঃ এটি মূলত উইন্ডোজের NTFS ফাইল সিস্টেমে ব্যবহৃত একটি কৌশল। এখানে একটি ফাইলের আড়ালে অন্য একটি ফাইলকে লুকিয়ে রাখা যায়। বাইরে থেকে ফাইলটির সাইজ বা নাম দেখে বোঝার উপায় থাকে না যে এর ভেতরে অন্য কিছু আছে।

৫. ডিস্ক পার্টিশন বা হিডেন ভলিউম (Hidden Partition) ঃ পুরো হার্ডড্রাইভের একটি নির্দিষ্ট অংশকে এমনভাবে লুকিয়ে ফেলা হয় যা সাধারণ অপারেটিং সিস্টেম বা ফাইল এক্সপ্লোরারে দেখা যায় না। বিশেষ সফটওয়্যার বা পাসওয়ার্ড ছাড়া এই অংশে প্রবেশ করা যায় না।

***** ২। ডাটা এনক্রিপশন অ্যালগরিদম এবং পদ্ধতি আলোচনা কর।**

বাকাশিবো- ২০২৫

উত্তর ঃ তথ্যকে সুরক্ষিত করার জন্য ডাটা এনক্রিপশন বর্তমানে অপরিহার্য। এটি মূলত গাণিতিক সূত্রের (Algorithm) মাধ্যমে সাধারণ তথ্যকে একটি গোপন কোডে রূপান্তর করে। নিচে প্রধান এনক্রিপশন অ্যালগরিদম এবং পদ্ধতিগুলো সহজ ভাষায় আলোচনা করা হলো ঃ

১. এনক্রিপশনের প্রধান পদ্ধতিসমূহ (Encryption Methods) ঃ

Key ব্যবহারের ওপর ভিত্তি করে এনক্রিপশন মূলত দুই প্রকার যথা ঃ

i) সিমেট্রিক এনক্রিপশন (Symmetric Encryption) ঃ এখানে তথ্য লক (এনক্রিপ্ট) এবং আনলক (ডিক্রিপ্ট) করার জন্য একই Key ব্যবহার করা হয়। এটি অত্যন্ত দ্রুত কাজ করে।

উদাহরণ ঃ হার্ডড্রাইভ এনক্রিপশন বা বড় ফাইল ট্রান্সফার।

ii) অ্যাসিমেট্রিক এনক্রিপশন (Asymmetric Encryption) ঃ এখানে দুটি আলাদা কবু থাকে। একটি 'পাবলিক কী' এবং একটি 'প্রাইভেট কী'।

উদাহরণ ঃ ডিজিটাল সিগনেচার, অনলাইন ব্যাংকিং, ব্রাউজিং নিরাপত্তা।

২. জনপ্রিয় এনক্রিপশন অ্যালগরিদমসমূহ (Common Algorithms) ঃ

i) AES (Advanced Encryption Standard) ঃ এটি বর্তমানে বিশ্বের সবচেয়ে শক্তিশালী এবং বহুল ব্যবহৃত অ্যালগরিদম। এটি একটি সিমেট্রিক পদ্ধতি।

বৈশিষ্ট্য ঃ এটি 128, 192 বা 256 বিট দৈর্ঘ্যের কি ব্যবহার করে। ব্যবহারঃ ওয়াইফাই নিরাপত্তা (WPA2), হোয়াটসঅ্যাপ মেসেজ এবং সরকারি তথ্য রক্ষা।

ii) DES (Data Encryption Standard) ঃ এটি 1970-এর দশকে তৈরি প্রথম দিকের অ্যালগরিদম। এটিও একটি সিমেট্রিক পদ্ধতি।

বৈশিষ্ট্য ঃ এর কি সাইজ মাত্র 56-বিট, যা বর্তমানে খুব সহজেই হ্যাক করা যায়। তাই এটি এখন আর ব্যবহৃত হয় না।

iii) RSA (Rivest-Shamir-Adleman) ঃ এটি একটি অত্যন্ত শক্তিশালী অ্যাসিমেট্রিক অ্যালগরিদম।

বৈশিষ্ট্য ঃ এটি বড় বড় মৌলিক সংখ্যা (Prime Numbers) ব্যবহার করে জটিল গাণিতিক সুরক্ষা তৈরি করে।

ব্যবহার ঃ ইমেইল নিরাপত্তা এবং ডিজিটাল সার্টিফিকেটে ব্যবহৃত হয়।

iv) 3DES (Triple DES) ঃ এটি পুরাতন DES-কে আরও শক্তিশালী করার একটি পদ্ধতি, যেখানে একই তথ্যকে তিনবার এনক্রিপ্ট করা হয়। যদিও এটি এখন AES-এর তুলনায় ধীরগতির।