জাতীয় বিশ্ববিদ্যালয়ের সিলেবাসভুক্ত আইসিটি বিষয়ক অনলাইন কোর্স
রিডিং ম্যাটেরিয়াল

৬.৩ ক্রিপ্টোগ্রাফির মৌলিক ধারণা

ক্রিপ্টোগ্রাফির ঐতিহাসিক পটভূমি:

ক্রিপ্টোগ্রাফির ইতিহাস অত্যন্ত প্রাচীন এবং রোমাঞ্চকর। এর সূচনা হয়েছিল প্রায় দুই হাজার বছর আগে, যখন গোপন যোগাযোগ ছিল রাজনৈতিক এবং সামরিক ক্ষমতার একটি গুরুত্বপূর্ণ উপাদান। এই প্রাচীন গোপন সংকেত পদ্ধতির সবচেয়ে বিখ্যাত উদাহরণ হলো **সিজার সাইফার (Caesar Cipher)**।

জুলিয়াস সিজার (Julius Caesar) ছিলেন রোমান সাম্রাজ্যের এক প্রভাবশালী সম্রাট, যিনি খ্রিস্টপূর্ব ৫০ অব্দের দিকে শাসন করতেন। যুদ্ধক্ষেত্রে তার সেনাবাহিনীর সাথে যোগাযোগ ছিল অত্যন্ত গুরুত্বপূর্ণ, কিন্তু শত্রুদের হাতে বার্তা পড়ে যাওয়ার ঝুঁকি ছিল সবসময়। এই সমস্যার সমাধান খুঁজতে গিয়ে সিজার একটি সরল কিন্তু কার্যকর পদ্ধতি আবিষ্কার করেন।

সিজারের পদ্ধতিটি ছিল অত্যন্ত সহজ: তিনি প্রতিটি অক্ষরকে বর্ণমালায় তিনটি স্থান এগিয়ে নিয়ে যেতেন। অর্থাৎ, অক্ষর A লেখা হতো D হিসেবে, B লেখা হতো E হিসেবে, C লেখা হতো F হিসেবে—এভাবে পুরো বার্তা জুড়ে। এই সরল স্থানান্তরের মাধ্যমে যেকোনো বার্তাকে সম্পূর্ণ দুর্বোধ্য করে ফেলা যেত।

একটি বাস্তব উদাহরণ দেখা যাক:

ধরুন, সিজার তার সেনাপতিদের এই বার্তা পাঠাতে চান: **"ATTACK AT DAWN"** (ভোরে আক্রমণ করো)
তিন স্থান এগিয়ে স্থানান্তরের পর বার্তাটি হয়ে যায়: **"DWWDFN DW GDZQ"**
শত্রুরা এই গোপন বার্তা হাতে পেলেও কিছুই বুঝতে পারত না। কিন্তু সিজারের সেনাপতিরা জানতেন যে প্রতিটি অক্ষরকে তিনটি স্থান পিছনে নিয়ে গেলেই মূল বার্তা উদ্ধার করা যাবে। এই পদ্ধতিতে D আবার A-তে রূপান্তরিত হতো, W হতো T, এবং এভাবে সম্পূর্ণ বার্তা পড়া যেত।
এই সহজ কিন্তু যুগান্তকারী পদ্ধতি আজও **"Caesar Cipher"** নামে পরিচিত এবং ক্রিপ্টোগ্রাফির ইতিহাসে প্রথম পরিচিত **Substitution Cipher** (প্রতিস্থাপন সাইফার) হিসেবে স্বীকৃত। যদিও আধুনিক মানদণ্ডে এই পদ্ধতি অত্যন্ত দুর্বল, তবুও এটি গোপন যোগাযোগের ভিত্তিপ্রস্তর স্থাপন করেছে এবং আজকের জটিল ক্রিপ্টোগ্রাফিক পদ্ধতির পূর্বসূরি।

আধুনিক সময়ে, সিজার সাইফার ব্যবহার করে আমরা শুধু তিন নয়, যেকোনো সংখ্যক স্থান (১ থেকে ২৫-এর মধ্যে) এগিয়ে বা পিছিয়ে অক্ষর স্থানান্তর করতে পারি। এই স্থানান্তরের সংখ্যাটিই হলো "শিফট (Shift)" বা চাবি। সঠিক শিফট সংখ্যা ছাড়া বার্তা পড়া অসম্ভব।

ক্রিপ্টোগ্রাফি কী এবং কেন গুরুত্বপূর্ণ?

ক্রিপ্টোগ্রাফি (Cryptography) হলো গোপন সংকেত ব্যবহার করে তথ্য বা ডেটা সুরক্ষিত রাখার একটি বৈজ্ঞানিক শাস্ত্র এবং প্রযুক্তিগত কৌশল। গ্রিক শব্দ "Kryptos" (অর্থ: গোপন) এবং "Graphein" (অর্থ: লেখা) থেকে এই শব্দটির উৎপত্তি। সহজ ভাষায়, ক্রিপ্টোগ্রাফি হলো এমন একটি পদ্ধতি যার মাধ্যমে কোনো তথ্যকে এমনভাবে রূপান্তরিত করা হয় যেন শুধুমাত্র প্রেরক এবং নির্দিষ্ট প্রাপক ছাড়া অন্য কেউ সেই তথ্য পড়তে বা বুঝতে না পারে।

ডিজিটাল যুগে ক্রিপ্টোগ্রাফির গুরুত্ব অপরিসীম। আমরা যখন অনলাইন ব্যাংকিং করি, ই-মেইল পাঠাই, সোশ্যাল মিডিয়ায় মেসেজ করি বা অনলাইনে কেনাকাটা করি—প্রতিটি ক্ষেত্রে ক্রিপ্টোগ্রাফি আমাদের তথ্য সুরক্ষিত রাখে। এটি নিশ্চিত করে যে আমাদের ব্যক্তিগত তথ্য, আর্থিক লেনদেন এবং গোপনীয় যোগাযোগ হ্যাকার বা অপরাধীদের হাতে পড়ে না।

ক্রিপ্টোগ্রাফির মৌলিক উপাদানসমূহ

ক্রিপ্টোগ্রাফি বুঝতে হলে কয়েকটি মৌলিক ধারণা সম্পর্কে স্পষ্ট জ্ঞান থাকা প্রয়োজন:

১. প্লেইন টেক্সট (Plain Text): এটি হলো মূল বার্তা বা তথ্য, যা সম্পূর্ণ পাঠযোগ্য এবং সবাই সহজেই বুঝতে পারে। উদাহরণস্বরূপ, "আমার পাসওয়ার্ড হলো ১২৩৪৫" এটি একটি প্লেইন টেক্সট। এই ধরনের তথ্য যদি অসুরক্ষিতভাবে পাঠানো হয়, তবে যে কেউ তা পড়ে ফেলতে পারে।

২. এনক্রিপশন (Encryption): এটি হলো প্লেইন টেক্সটকে একটি বিশেষ গাণিতিক প্রক্রিয়ার মাধ্যমে দুর্বোধ্য বা কোডেড বার্তায় রূপান্তর করার কৌশল। এনক্রিপশন প্রক্রিয়ায় একটি বিশেষ চাবি (Key) ব্যবহার করা হয়, যা তথ্যকে সুরক্ষিত করে। এটি অনেকটা একটি তালা দিয়ে বাক্স বন্ধ করার মতো। এনক্রিপশনের মাধ্যমে তথ্য এমনভাবে পরিবর্তিত হয় যে সঠিক চাবি ছাড়া কেউ তা পড়তে পারে না।

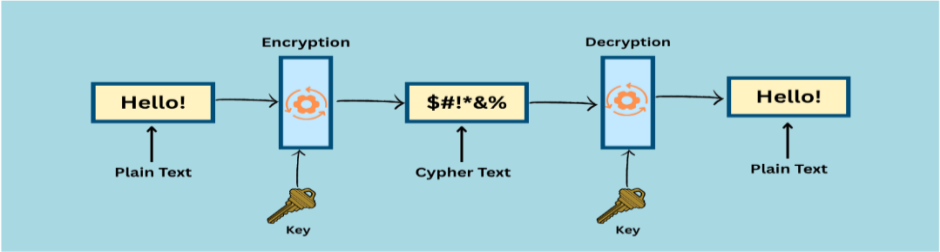
৩. সাইফার টেক্সট (Ciphertext): এনক্রিপ্ট করার পর যে দুর্বোধ্য বা এলোমেলো দেখতে বার্তাটি তৈরি হয়, তাকে সাইফার টেক্সট বলে। উদাহরণস্বরূপ, "আমার পাসওয়ার্ড হলো ১২৩৪৫" এনক্রিপ্ট করার পর হতে পারে "%aGf@jK৯&bNm#২xPq"। এই সাইফার টেক্সট দেখে কেউ বুঝতে পারবে না এর ভেতরে আসলে কী বার্তা লুকিয়ে আছে।

৪. ডিক্রিপশন (Decryption): এটি হলো এনক্রিপশনের বিপরীত প্রক্রিয়া। ডিক্রিপশনের মাধ্যমে সাইফার টেক্সটকে আবার মূল প্লেইন টেক্সটে ফিরিয়ে আনা হয়। এই কাজটি করতেও সঠিক চাবি প্রয়োজন। এটি অনেকটা তালা খোলার মতো—সঠিক চাবি থাকলেই শুধু বার্তা পড়া যাবে।

৫. কী (Key): কী হলো ক্রিপ্টোগ্রাফির সবচেয়ে গুরুত্বপূর্ণ উপাদান। এটি একটি গোপন তথ্য, অনেকটা পাসওয়ার্ডের মতো, যা ডেটাকে এনক্রিপ্ট (লক) এবং ডিক্রিপ্ট (আনলক) করতে ব্যবহৃত হয়। কী-এর জটিলতা এবং দৈর্ঘ্য যত বেশি হয়, নিরাপত্তা তত শক্তিশালী হয়। সঠিক কী ছাড়া কেউ সাইফার টেক্সটকে প্লেইন টেক্সটে রূপান্তর করতে পারে না। আধুনিক ক্রিপ্টোগ্রাফিতে কী-এর দৈর্ঘ্য ১২৮, ২৫৬ বা তারও বেশি বিট হতে পারে।

ক্রিপ্টোগ্রাফির সম্পূর্ণ প্রক্রিয়াটি এভাবে সংক্ষেপে প্রকাশ করা যায়:

Plain Text → (Encryption with a Key) → Ciphertext → (Decryption with the Same/Related Key) → Plain Text



উদাহরণস্বরূপ:

- **প্রেরক:** "ব্যাংক অ্যাকাউন্ট নম্বর: ১২৩৪৫৬৭৮৯০" (প্লেইন টেক্সট)
- **এনক্রিপশন:** একটি শক্তিশালী কী ব্যবহার করে এনক্রিপ্ট করা হলো
- **পাঠানো বার্তা:** "9Kf#mL2@pR7&nB5%" (সাইফার টেক্সট)
- **প্রাপক:** সঠিক কী ব্যবহার করে ডিক্রিপ্ট করলেন
- **প্রাপ্ত বার্তা:** "ব্যাংক অ্যাকাউন্ট নম্বর: ১২৩৪৫৬৭৮৯০" (পুনরায় প্লেইন টেক্সট)

এই পুরো প্রক্রিয়ায় যদি কোনো অপরাধী বা হ্যাকার মাঝপথে সাইফার টেক্সট হাতে পায়, তবুও সঠিক কী না থাকায় সে মূল তথ্য পড়তে পারবে না।

এনক্রিপশনের প্রকারভেদ: সিমেট্রিক ও অ্যাসিমেট্রিক

কী-এর ব্যবহার এবং কাঠামোর উপর ভিত্তি করে এনক্রিপশন প্রধানত দুই প্রকার: সিমেট্রিক এনক্রিপশন (Symmetric Encryption) এবং অ্যাসিমেট্রিক এনক্রিপশন (Asymmetric Encryption)। এই দুই ধরনের এনক্রিপশন ভিন্ন ভিন্ন পরিস্থিতিতে ব্যবহৃত হয় এবং প্রতিটির নিজস্ব সুবিধা ও অসুবিধা রয়েছে।

১. সিমেট্রিক এনক্রিপশন (Symmetric Encryption)

সিমেট্রিক এনক্রিপশন পদ্ধতিতে ডেটা লক (এনক্রিপ্ট) এবং আনলক (ডিক্রিপ্ট) করার জন্য একই চাবি (Key) ব্যবহার করা হয়। এটি অনেকটা আপনার ঘরের তালার মতো—একই চাবি দিয়ে আপনি দরজা বন্ধ এবং খোলেন।

কীভাবে কাজ করে:

ধরুন, আপনি আপনার বন্ধুকে একটি গোপন বার্তা পাঠাতে চান। আপনি একটি চাবি (পাসওয়ার্ড) ব্যবহার করে বার্তাটি এনক্রিপ্ট করলেন। এখন আপনার বন্ধু সেই বার্তা পড়তে হলে তার কাছেও ঠিক একই চাবির একটি কপি থাকতে হবে। শুধুমাত্র সেই চাবি দিয়েই সে বার্তাটি ডিক্রিপ্ট করে পড়তে পারবে।

সুবিধা	অসুবিধা
• অত্যন্ত দ্রুত এবং কার্যকর • বড় পরিমাণ ডেটা এনক্রিপ্ট করার জন্য উপযুক্ত • কম্পিউটেশনাল খরচ কম	• প্রধান সমস্যা হলো চাবি শেয়ার করা। আপনাকে নিরাপদভাবে চাবিটি আপনার বন্ধুর কাছে পৌঁছে দিতে হবে, যা ঝুঁকিপূর্ণ হতে পারে • যদি চাবিটি কোনো তৃতীয় পক্ষের হাতে চলে যায়, তবে সমস্ত যোগাযোগ অসুরক্ষিত হয়ে পড়ে

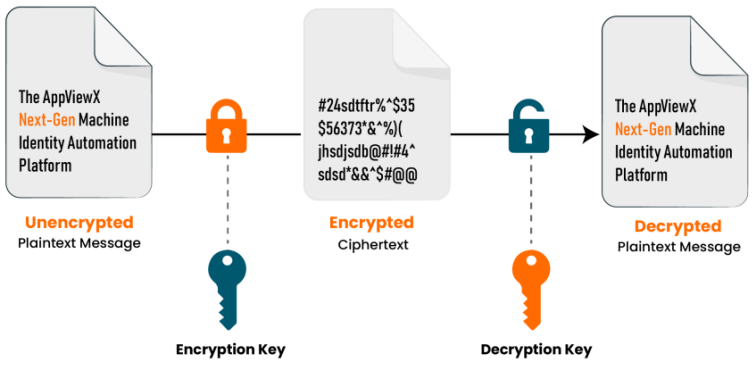
২. অ্যাসিমেট্রিক এনক্রিপশন (Asymmetric Encryption)

অ্যাসিমেট্রিক এনক্রিপশন পদ্ধতিতে একজোড়া চাবি ব্যবহার করা হয়: একটি **পাবলিক কী (Public Key)** এবং একটি **প্রাইভেট কী (Private Key)**। এই দুটি চাবি গাণিতিকভাবে একে অপরের সাথে সম্পর্কযুক্ত কিন্তু সম্পূর্ণ আলাদা। এই পদ্ধতিকে "Public Key Cryptography" বা "Public Key Infrastructure (PKI)" ও বলা হয়।

দুই ধরনের চাবি:

ক. পাবলিক কী (Public Key): এই চাবিটি সবার জন্য উন্মুক্ত এবং প্রকাশ্য। যে কেউ আপনার পাবলিক কী ব্যবহার করে ডেটা এনক্রিপ্ট (লক) করে আপনাকে পাঠাতে পারে। এটি অনেকটা আপনার বাসার ঠিকানার মতো, যা সবাই জানতে পারে এবং কেউ আপনাকে চিঠি পাঠাতে পারে।

খ. প্রাইভেট কী (Private Key): এই চাবিটি সম্পূর্ণ গোপন এবং শুধুমাত্র আপনার কাছেই থাকে। পাবলিক কী দিয়ে লক করা যেকোনো ডেটা শুধুমাত্র আপনার প্রাইভেট কী দিয়েই আনলক (ডিক্রিপ্ট) করা সম্ভব। এটি অনেকটা আপনার ঘরের চাবির মতো, যা শুধু আপনিই রাখেন।



কীভাবে কাজ করে:

ধরুন, আপনার বন্ধু আপনাকে একটি গোপন বার্তা পাঠাতে চায়। প্রক্রিয়াটি এভাবে সম্পন্ন হয়:

১. আপনি আপনার পাবলিক কী সবার সাথে শেয়ার করেন (ইন্টারনেটে প্রকাশ করেন)

২. আপনার বন্ধু আপনার পাবলিক কী ব্যবহার করে তার বার্তাটি এনক্রিপ্ট (লক) করে

৩. এনক্রিপ্ট করা বার্তাটি আপনার কাছে পাঠায় ৪. আপনি আপনার গোপন প্রাইভেট কী দিয়ে সেই বার্তা ডিক্রিপ্ট (আনলক) করে পড়েন

যেহেতু প্রাইভেট কী শুধু আপনার কাছেই আছে, তাই অন্য কেউ—এমনকি যিনি বার্তাটি পাঠিয়েছেন তিনিও—এই বার্তা পড়তে পারবেন না।

সুবিধা	**অসুবিধা**
• চাবি শেয়ার করার ঝুঁকি নেই, কারণ প্রাইভেট কী কখনও কারও সাথে শেয়ার করতে হয় না • অত্যন্ত নিরাপদ • ডিজিটাল সিগনেচার এবং পরিচয় যাচাইয়ের জন্য উপযুক্ত	• সিমেট্রিক এনক্রিপশনের তুলনায় অনেক ধীর • বেশি কম্পিউটেশনাল শক্তি প্রয়োজন • বড় ডেটা এনক্রিপ্ট করতে সময়সাপেক্ষ

বাস্তব ব্যবহার:
আধুনিক সিস্টেমে প্রায়ই এই দুই ধরনের এনক্রিপশন একসাথে ব্যবহার করা হয়। যেমন, HTTPS প্রোটোকলে প্রথমে অ্যাসিমেট্রিক এনক্রিপশন ব্যবহার করে একটি সিমেট্রিক কী নিরাপদে শেয়ার করা হয়, তারপর সেই সিমেট্রিক কী দিয়ে দ্রুত ডেটা আদান-প্রদান করা হয়। এটি "হাইব্রিড এনক্রিপশন" নামে পরিচিত।
হ্যাশ ফাংশন: ডিজিটাল ফিঙ্গারপ্রিন্ট

হ্যাশ (Hash) বা হ্যাশ ফাংশন হলো ক্রিপ্টোগ্রাফির আরেকটি অত্যন্ত গুরুত্বপূর্ণ উপাদান। এটি যেকোনো ডিজিটাল ডেটার (যেমন: একটি ফাইল, পাসওয়ার্ড, বা মেসেজ) একটি অনন্য "ডিজিটাল ফিঙ্গারপ্রিন্ট" তৈরি করে। হ্যাশ ফাংশন এনক্রিপশন নয়, বরং এটি একটি একমুখী গাণিতিক প্রক্রিয়া।

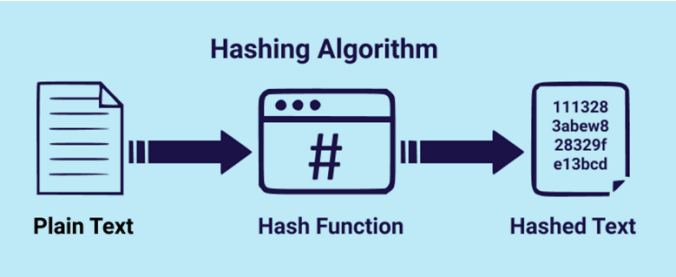
হ্যাশের মূল বৈশিষ্ট্যসমূহ

১. নির্দিষ্ট দৈর্ঘ্য (Fixed Length): মূল ডেটা যত ছোট বা বড় হোক না কেন, হ্যাশ সবসময় একটি নির্দিষ্ট দৈর্ঘ্যের হয়। উদাহরণস্বরূপ, SHA-২৫৬ হ্যাশ অ্যালগরিদম সবসময় ২৫৬ বিট বা ৬৪ ক্যারেক্টারের একটি হ্যাশ তৈরি করে, তা একটি ছোট শব্দ হোক কিংবা একটি সম্পূর্ণ বই।

২. অনন্য এবং সংবেদনশীল (Unique and Sensitive): মূল ডেটার সামান্যতম পরিবর্তন—এমনকি একটি কমা বা স্পেস বদল করলেও—সম্পূর্ণ নতুন এবং ভিন্ন একটি হ্যাশ তৈরি হয়। উদাহরণ:

- "Hello World" এর হ্যাশ: a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

- "Hello World." (শুধু একটি পিরিয়ড যোগ) এর হ্যাশ: c0535e4be2b79ffd93291305436bf889314e4a3faec05ecffcbb7df31ad9e51a



৩. একমুখী প্রক্রিয়া (One-Way Function): হ্যাশ থেকে মূল ডেটায় ফেরত যাওয়া প্রায় অসম্ভব। এটি একটি একমুখী রাস্তার মতো। একবার ডেটা হ্যাশ হয়ে গেলে, সেই হ্যাশ থেকে মূল ডেটা উদ্ধার করা যায় না। এটি অনেকটা ফলের জুস তৈরি করার মতো—একবার জুস হয়ে গেলে আবার আস্ত ফল ফিরে পাওয়া সম্ভব নয়।

৪. দ্রুততা (Fast Computation): হ্যাশ তৈরি করা অত্যন্ত দ্রুত প্রক্রিয়া। যেকোনো আকারের ডেটা মুহূর্তেই হ্যাশ করা যায়।

হ্যাশের ব্যবহার

১. ডেটা অখণ্ডতা যাচাই (Data Integrity Verification): হ্যাশের প্রধান ব্যবহার হলো কোনো ফাইল বা ডকুমেন্ট পরিবর্তিত হয়েছে কিনা তা যাচাই করা। যদি দুটি ফাইলের হ্যাশ হুবহু মিলে যায়, তার মানে ফাইল দুটিও হুবহু এক এবং এতে কোনো পরিবর্তন করা হয়নি।

উদাহরণ: আপনি একটি সফটওয়্যার ডাউনলোড করলেন। ওয়েবসাইটে ফাইলের হ্যাশ দেওয়া আছে। ডাউনলোডের পর আপনি ফাইলটির হ্যাশ নিজে তৈরি করে মিলিয়ে দেখতে পারেন। যদি দুটি হ্যাশ মিলে যায়, তার মানে ফাইলটি সম্পূর্ণ এবং কেউ এতে ম্যালওয়্যার যুক্ত করেনি।

২. পাসওয়ার্ড সংরক্ষণ (Password Storage): ওয়েবসাইট এবং অ্যাপ্লিকেশনগুলো আপনার আসল পাসওয়ার্ড সংরক্ষণ করে না, বরং পাসওয়ার্ডের হ্যাশ সংরক্ষণ করে। যখন আপনি লগইন করেন, আপনার দেওয়া পাসওয়ার্ডের হ্যাশ তৈরি করে সংরক্ষিত হ্যাশের সাথে মিলিয়ে দেখা হয়। এতে ডাটাবেস হ্যাক হলেও আসল পাসওয়ার্ড ফাঁস হয় না।

৩. ডিজিটাল সিগনেচার (Digital Signature): ডিজিটাল সিগনেচারে হ্যাশ অত্যন্ত গুরুত্বপূর্ণ ভূমিকা পালন করে। সম্পূর্ণ ডকুমেন্ট এনক্রিপ্ট না করে, শুধু ডকুমেন্টের হ্যাশ এনক্রিপ্ট করা হয়, যা অনেক দ্রুত এবং কার্যকর।

৪. ব্লকচেইন টেকনোলজি (Blockchain): ক্রিপ্টোকারেন্সি এবং ব্লকচেইনে প্রতিটি ব্লকের হ্যাশ তৈরি করা হয় যা পরবর্তী ব্লকের সাথে সংযুক্ত থাকে, এভাবে একটি অপরিবর্তনীয় চেইন তৈরি হয়।

জনপ্রিয় হ্যাশ অ্যালগরিদম

- **MD5 (Message Digest 5):** পুরনো এবং এখন নিরাপদ নয়, তবে এখনও কিছু ক্ষেত্রে ব্যবহৃত হয়
- **SHA-1 (Secure Hash Algorithm 1):** আগে জনপ্রিয় ছিল কিন্তু এখন দুর্বল বলে বিবেচিত

- **SHA-256 এবং SHA-512:** বর্তমানে সবচেয়ে নিরাপদ এবং ব্যাপকভাবে ব্যবহৃত
- **SHA-3:** সর্বশেষ এবং সবচেয়ে শক্তিশালী হ্যাশ অ্যালগরিদম

এই পাঠে যে বিষয়গুলো আলোচনা করা হয়েছে:

১. ক্রিপ্টোগ্রাফির ইতিহাস ও সিজার সাইফার (Caesar Cipher)

২. ক্রিপ্টোগ্রাফির মৌলিক উপাদানসমূহ (প্লেইন টেক্সট, এনক্রিপশন, সাইফার টেক্সট, ডিক্রিপশন, কী)

৩. এনক্রিপশনের প্রকারভেদ: সিমেট্রিক ও অ্যাসিমেট্রিক এনক্রিপশন

৪. হ্যাশ ফাংশন (Hash Function)

৫. হ্যাশের ব্যবহার (ডেটা অখণ্ডতা যাচাই, পাসওয়ার্ড সংরক্ষণ, ডিজিটাল সিগনেচার)

এছাড়াও নিচের বিষয়গুলো সম্পর্কে বিশদভাবে জানতে ভিজিট করুন:

Cryptography Basics & Caesar Cipher:

a) https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher

Symmetric vs Asymmetric Encryption:

a) https://www.youtube.com/watch?v=AQDCe৫৮৫Lnc

b)https://www.ssltrust.com.au/learning/ssl/symmetric-vs-asymmetric-encryption

Hashing Algorithms (SHA-256):

a) https://www.youtube.com/watch?v=jmtzX-NPFDc