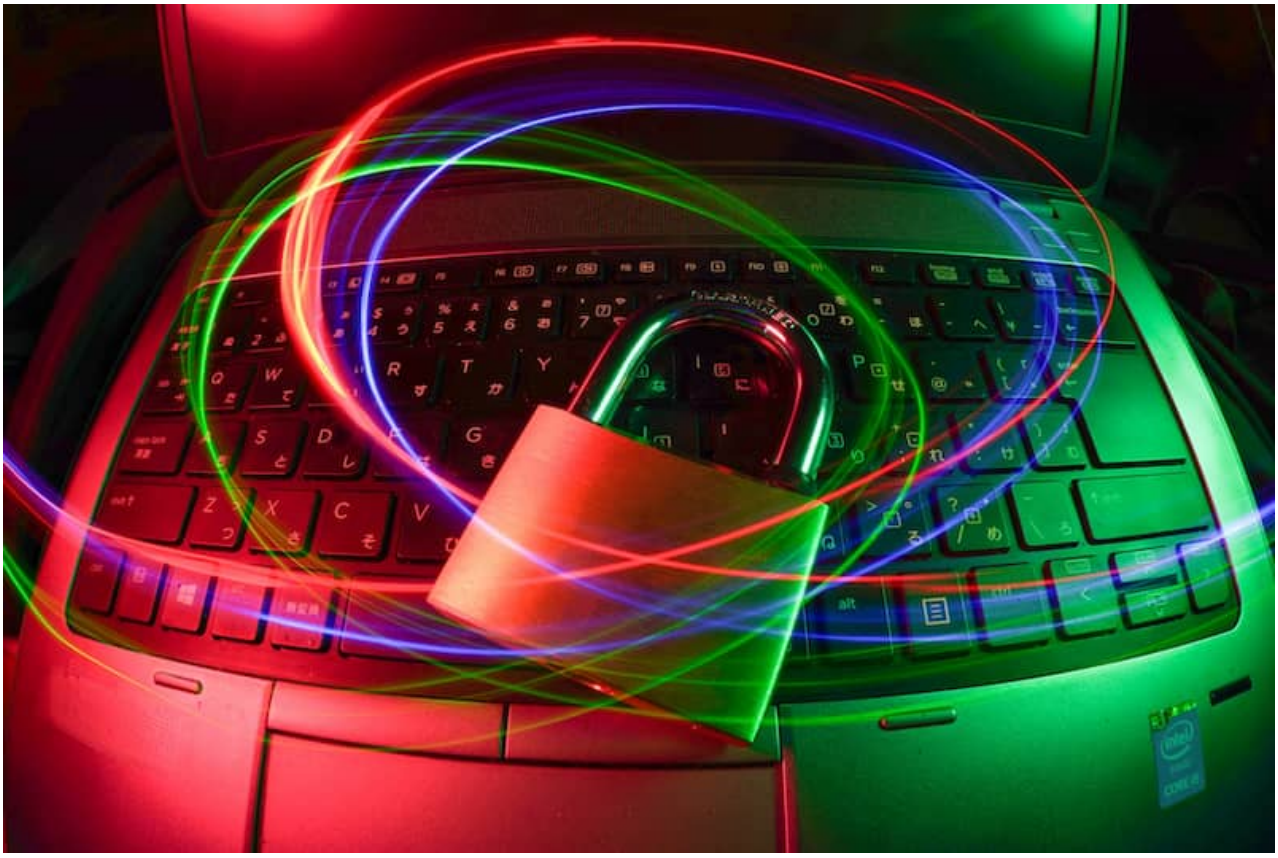
এনক্রিপশন কী? এটা কী কাজে লাগে?



এনক্রিপশন এক ধরনের প্রযুক্তি। আপনার পছন্দের ডিভাইস ব্যবহার করে সেন্ড করা, রিসিভ করা বা জমা করা ডাটার সুরক্ষা প্রদান করতে পারে এনক্রিপশন। ফোনে থাকা টেক্সট মেসেজ থেকে শুরু করে ব্যাংকিং তথ্য পর্যন্ত সবকিছুর নিরাপত্তা প্রদান করতে পারে এনক্রিপশন প্রযুক্তি।

এনক্রিপশন সম্পর্কে অনেকের মধ্যেই আগ্রহ ও আকর্ষণের কোনো সীমা নেই। চলুন জেনে নেওয়া যাক এনক্রিপশন সম্পর্কে বিস্তারিত। এই পোস্টে জানবেনঃ

- এনক্রিপশন কী
- এনক্রিপশন কীভাবে কাজ করে
- এনক্রিপশন কেনো গুরুত্বপূর্ণ
- এনক্রিপশন এর অসুবিধাসমূহ

এনক্রিপশন কী?

এনক্রিপশন হলো এমন একটি প্রক্রিয়া যেখানে কোনো ফাইলকে এমন ফরম্যাটে পরিবর্তিত করা হয়, যা শুধুমাত্র সিক্রেট কোড বা ডিক্রিপশন কি এক্সেস করা যাবে। এটি সেনসিটিভ ইনফরমেশনে নিরাপত্তা প্রদান করে।

ব্যবহারকারীদের ব্যক্তিগত তথ্য বিভিন্ন ওয়েবসাইট ও সার্ভারে অনলাইনে জমা হয়ে থাকে। আর এসব ডাটা সরাসরি সাধারণ টেক্সট ল্যাংগুয়েজে সংরক্ষণ না করে বরং একটি প্যাটার্নে সেভ করা হয়, যা শুধুমাত্র ড্রিক্রিপশন কি ব্যবহার করেই দেখা সম্ভব। অর্থাৎ অনলাইন বা অফলাইনে থাকা বিভিন্ন তথ্যের নিরাপত্তা রক্ষার উপাদান হলো

এনক্রিপশন। এনক্রিপশনের মাধ্যমে তথ্যকে বিক্ষিপ্ত উপাত্তে পরিণত করা হয় যা দেখে কোনো মর্ম উদ্ধার করা যায়না। কিন্তু নির্দিষ্ট একটি “ডিক্রিপশন কি” ব্যবহার করে ঐ এনক্রিপ্টেড তথ্য পুনরায় আগের মত করে তোলা সম্ভব। এনক্রিপশনের বিপরীত হল “ডিক্রিপশন”।

এনক্রিপশন কীভাবে কাজ করে?

এনক্রিপশন হলো এমন একটি প্রক্রিয়া যেখানে ইমেইল বা টেক্সট মেসেজ এর মতো প্লেইন টেক্সট একটি অপাঠযোগ্য ফরম্যাটে পরিণত করা হয়, যাকে বলা হচ্ছে “সাইফার টেক্সট।” কম্পিউটারে থাকা বা ইন্টারনেটে পাঠানো বা জমা থাকা ডিজিটাল ডাটার গোপনীয়তা রক্ষা করতে এনক্রিপশন ব্যবহৃত হয়।

-

এনক্রিপশন ব্যবহার করে পাঠানো মেসেজ যখন কাংখিত ব্যক্তির কাছে পৌঁছায়, তখন সেটি সাধারণ রূপে পরিণত হয়। এই মেসেজ আনলক করতে সেন্ডার ও রিসিভার, উভয়ের কাছেই একটি গোপন এনক্রিপশন কি রয়েছে, যা স্বয়ংক্রিয়ভাবে কাজ করে।

এনক্রিপশন এর ধরন

বিভিন্ন প্রয়োজন ও নিরাপত্তাকে মাথায় রেখে বিভিন্ন ধরনের এনক্রিপশন তৈরি করা হয়েছে। চলুন জেনে নেওয়া যাক কিছু জনপ্রিয় এনক্রিপশনের উদাহরণ সম্পর্কে।

ডাটা এনক্রিপশন স্ট্যান্ডার্ড

ডাটা এনক্রিপশন স্ট্যান্ডার্ড বা ডিইএস (DES) হল একটি ব্যাসিক-লেভেল এনক্রিপশন স্ট্যান্ডার্ড। ১৯৭০ দশকে আইবিএম এটি ডিজাইন করে। প্রযুক্তিগত উন্নতি ও হার্ডওয়্যার এর মূল্যহ্রাস হওয়ার ফলে এটি সেনসিটিভ ডাটা প্রদানে বেশ দূর্বল হয়ে পড়েছে। এটি ৫৬ বিট এনক্রিপশন প্রযুক্তি।

ট্রিপল ডিইএস

ট্রিপল ডিইএস মূলত তিনটি ৫৬ বিট কি ব্যবহার করে যা অরিজিনাল ডিইএসের চেয়ে ৩গুণ সুরক্ষা প্রদান করে। তবে বর্তমানে এটিও খুব একটা ব্যবহৃত হচ্ছেনা।

আরএসএ

তিনজন কম্পিউটার সাইন্টিস্ট (Rivest-Shamir-Adleman) এর নামের প্রথম অক্ষর অনুসারে তৈরি আরএসএ একটি এনক্রিপশন পদ্ধতি, যা শক্তিশালী ও জনপ্রিয় এনক্রিপশন ব্যবহার করে থাকে। নিরাপদে ডাটা আদানপ্রদান এটি ব্যাপকভাবে ব্যবহৃত হয়।

এডভান্সড এনক্রিপশন স্ট্যান্ডার্ড (এইএস)

এডভান্সড এনক্রিপশন স্ট্যান্ডার্ড বা এইএস হলো যুক্তরাষ্ট্র সরকার কতৃক ব্যবহৃত এনক্রিপশন মেথড, যা ১৯৯৮ সালে প্রথম প্রকাশ করা হয়। বিশ্বব্যাপী এটি ব্যাপকহারে ব্যবহৃত হয়।

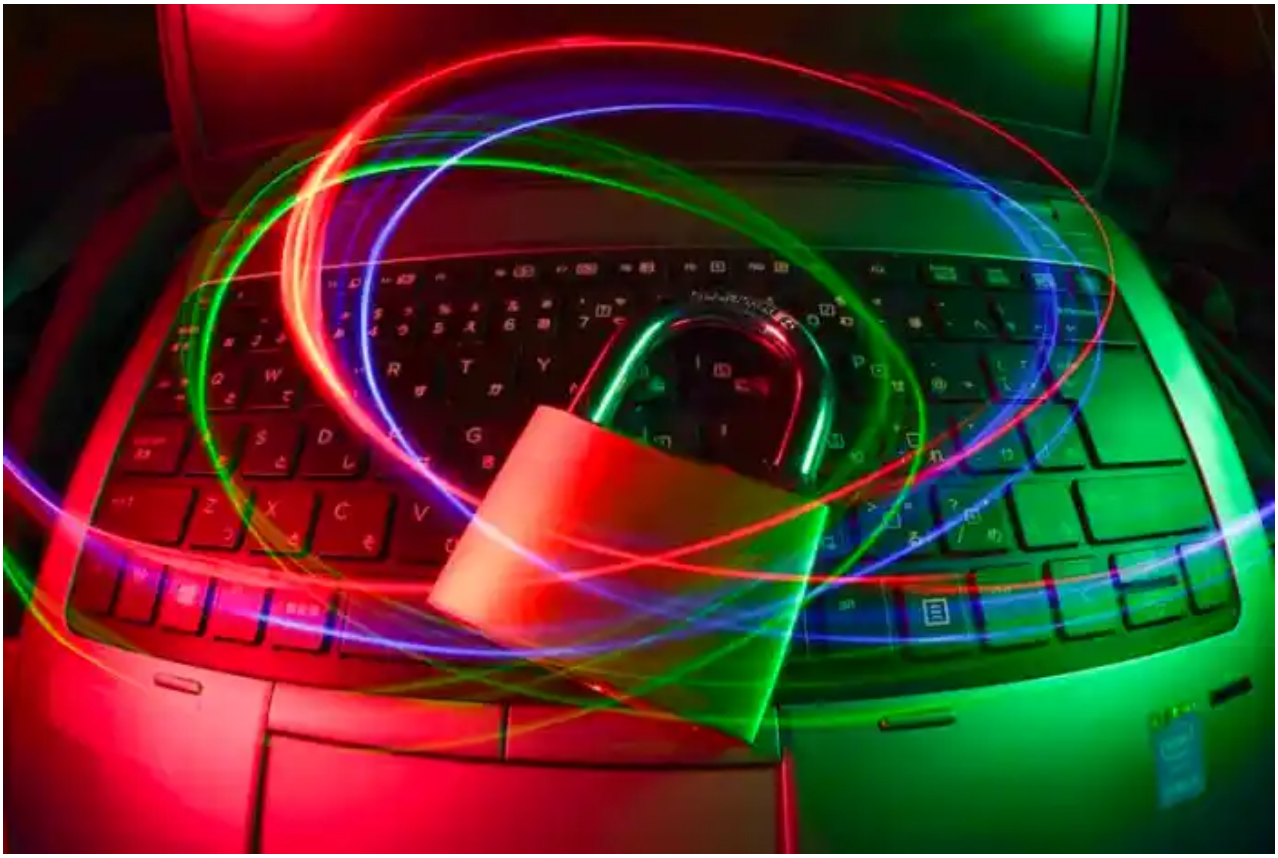
টুফিশ

টুফিশ অন্যতম দ্রুত এনক্রিপশন এলগরিদম এবং অনেক ক্ষেত্রে এটি অন্যদের চেয়ে একটু বেশিই দ্রুতগতির। এটি ফ্রি হওয়ায় যেকেউ বিনামূল্যে সফটওয়্যার ও হার্ডওয়্যারে ব্যবহার করতে পারে।

এসএসএল

বেশিরভাগ ওয়েবসাইটের ডাটা এনক্রিপ্ট করার মাধ্যমে সুরক্ষা প্রদান করে “সিকিউর সকেটস লেয়ার” বা এসএসএল। এটি ট্রানজিটে থাকা ডাটা লিক হওয়া থেকে ওয়েবসাইটকে রক্ষা করে।

কোনো ওয়েবসাইটে প্রবেশের পর ইউআরএল বারে প্যাডলক আইকন থাকলে ও https:// এর s আছে মানে উক্ত ওয়েবসাইট এনক্রিপশন প্রযুক্তি ব্যবহার করছে। অর্থাৎ এই সাইট থেকে আপনার কাছে যে তথ্য আসছে এবং আপনার কাছ থেকে এই সাইটে যে তথ্য যাচ্ছে সেগুলো পথিমধ্যে অন্য কেউ দেখতে পারবেনা। ইন্টারনেট সেবাদাতা প্রতিষ্ঠানও সেই তথ্য পাবেনা।



এনক্রিপশন কেনো গুরুত্বপূর্ণ

ইন্টারনেটের দুনিয়ায় এনক্রিপশন ভীষণ গুরুত্বপূর্ণ একটি বিষয়। চলুন এনক্রিপশন এর গুরুত্ব সম্পর্কে জানা যাক।

ইন্টারনেট প্রাইভেসি

এনক্রিপশন এর মাধ্যমে ব্যক্তিগত তথ্য কাংখিত ব্যক্তি/ডিভাইস ছাড়া অন্যদের কাছে প্রদর্শিত হয়না। যার ফলে সর্বোচ্চ স্তরের সুরক্ষা পাওয়া যায় এনক্রিপশন প্রযুক্তি ব্যবহার করে।

তবে এই বিষয়টি আপনার নিজেকেই নিশ্চিত করতে হবে। পাঠানো ইমেইলসমূহ এনক্রিপটেড কানেকশন ব্যবহার করে প্রেরণ নিশ্চিত করা অনলাইন প্রাইভেসির প্রথম শর্ত।

প্রায় প্রতিটি ইমেইল ক্লায়েন্টের সেটিংসে এনক্রিপশনের জন্য আলাদা সেটিংস দেওয়া থাকে। আপনার মেইল যদি ওয়েব ব্রাউজার থেকে চেক করেন, তবে ভিজিটের পর ওয়েবসাইটে এসএসএল এনক্রিপশন আছে কিনা, তা নিশ্চিতের দায়িত্ব আপনার।

একটি ব্যবসাকে হ্যাক করা

একাধিক আন্তর্জাতিক সংস্থা দ্বারা চালিত সাইবারক্রাইম বর্তমানে গ্লোবাল বিজনেসে পরিণত হয়েছে। বড় স্কেলের ডাটা লিকগুলো অনেক ক্ষেত্রে এই এনক্রিপশন প্রযুক্তি অকার্যকর হয়ে উঠার কারণে সৃষ্টি হয়।

আইনের প্রয়োগ

এনক্রিপশন ব্যবহার করে আইনের নিয়ম ও স্ট্যান্ডার্ডসমূহ মেনে চলা রাষ্ট্রের নাগরিকদের কর্তব্য। এছাড়াও কাস্টমারদের ডাটার নিরাপত্তার লক্ষ্যেও এটি ব্যবহৃত হয়।

এনক্রিপশন এর অসুবিধা

আমাদের ডাটার সুরক্ষার জন্য তৈরি করা হলেও চাইলে এনক্রিপশনকে আমাদের বিরুদ্ধে ব্যবহার করা যেতে পারে।

সাইবার ক্রিমিনালরা এনক্রিপশনের মাধ্যমে ডিভাইস লক করে দেয় ও অর্থ দাবি করে – এমন র‍্যানসামওয়্যার এর ঘটনা কিন্তু নতুন নয়। শুধুমাত্র ব্যক্তি নয়, প্রতিষ্ঠান পর্যায়েও ক্ষতি সাধনে সক্ষম এই র‍্যানসমওয়্যার। এছাড়াও অনেকসময় নির্দিষ্ট কম্পিউটারে র‍্যানসমওয়্যার অ্যাটাক চালানো হয়।

আক্রমণকারীরা কম্পিউটার, সার্ভারসহ বিভিন্ন ধরনের ডিভাইস এনক্রিপ্ট করার চেষ্টা করে সিস্টেমে র‍্যানসমওয়্যার ঢুকিয়ে। মাঝেমধ্যে এনক্রিপটেড ডাটার এনক্রিপশন কি প্রদানের আগে র‍্যানসমওয়্যারের অর্থ চাওয়া হয়।