থ্রিমা অ্যাপ ও কমপিউটার এনক্রিপশন

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

আমরা ইতোমধ্যেই জেনে গেছি গুলশানে জঙ্গি হামলার ছবি 'থ্রিমা' নামে একটি মেসেজিং সফটওয়্যারের মাধ্যমে ইন্টারনেটে ছড়িয়ে দেয়া হয়। এর আগেও থ্রিমা সফটওয়্যার ব্যবহার নিয়ে জঙ্গি সংগঠন আইএসের সম্পৃক্ততার কথা জানা যায়। এই রিপোর্টে দাবি করা হয়, আইএস তার সদস্যদের মধ্যে মেসেজিংয়ের জন্য এই অ্যাপটি ব্যবহার করে থাকে। আসলে এই অ্যাপটির এনক্রিপশন ম্যাকানিজম ও বার্তা মুছে দেয়ার অপশনের জন্য জঙ্গিদের কাছে বেশি জনপ্রিয়।

থ্রিমাকে সাধারণত খুবই নিরাপদ মেসেজিংয়ের অ্যাপ্লিকেশন হিসেবে মনে করা হয়। এটি ব্যবহার করে বার্তা পাঠানোর পর তা সার্ভার থেকে মুছে ফেলতে পারে। পরিচয় গোপন রেখে এটি করা যায় বলে ব্যবহারকারীকে শনাক্ত করা যায় না। আর এ কারণেই ওই রাতে কী ঘটেছিল, সে তথ্য পাওয়ার বিষয়টি বাংলাদেশের সংশ্লিষ্ট কর্তৃপক্ষকে কঠিন করে তুলেছে।

থ্রিমা ও আইএস : তথ্য নিরাপত্তাবিষয়ক এসসি ম্যাগাজিন এ বছরের ফেব্রুয়ারিতে থ্রিমা ও আইএসের সম্পর্ক নিয়ে একটি প্রতিবেদন প্রকাশ করে। প্রতিবেদনে বলা হয়, আইএসের হ্যাকিং ইউনিট সাইবার ক্যালিফেট তাদের যোগাযোগের জন্য টেলিগ্রাম ছেড়ে থ্রিমাতে চলে এসেছে। মিডল ইস্ট মিডিয়া রিসার্চ ইনস্টিটিউটের (এমইআরই) নির্বাহী পরিচালক স্টিভেন স্টালিনিস্কির বরাতে ওই প্রতিবেদনে বলা হয়, সাইবার ক্যালিফেট তাদের সমর্থনকারীদের থ্রিমা ব্যবহারের কথা বলে।

এরপর তাদের টেলিগ্রাম অ্যাকাউন্ট বন্ধ করে দেয়া হয়। এ বছরের জানুয়ারিতে সাইবার ক্যালিফেট নতুন নীতিমালা ঘোষণা করে, যাতে তাদের অনুসারীদের বিশ্বাসযোগ্য সূত্র ছাড়া কোনো লিঙ্কে ক্লিক করতে, টুইটারে সরাসরি বার্তা পাঠাতে এমনকি সামাজিক যোগাযোগের ওয়েবসাইট ব্যবহারে নিষেধ করা হয়। এর পরিবর্তে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক তথা ভিপিএন বা টর ব্যবহারে পরামর্শ দেয়া হয়।

থ্রিমা কী : বিজনেস ইনসাইডারের তথ্য অনুযায়ী, থ্রিমা জার্মানির একটি জনপ্রিয় অ্যাপ। আইওএস, অ্যান্ড্রয়িড ও উইন্ডোজ অপারেটিং সিস্টেমের ফোনে থ্রিমা ব্যবহার করে বার্তা বিনিময় ছাড়াও মাল্টিমিডিয়া, লোকেশন, ভয়েস মেসেজ ও ফাইল পাঠানো যায়। সুইজারল্যান্ডের সফটওয়্যার নির্মাতা প্রতিষ্ঠান থ্রিমা জিএমবিএইচ ২০১২ সালে এটি তৈরি করে। এর সার্ভার সুইজারল্যান্ডে। ২০১৫ সালের জুন মাসের তথ্য অনুযায়ী, ৩৫ লাখ ব্যবহারকারী থ্রিমা ব্যবহার করে, যার বেশিরভাগ জার্মান। থ্রিমা তৈরির পেছনে কাজ করছে ম্যানুয়েল ক্যাসপার নামে এক উদ্যোক্তা প্রতিষ্ঠান। আগে প্রতিষ্ঠানটির নাম ছিল ক্যাসপার সিস্টেমস। সফটওয়্যার নির্মাতা মার্টিন ব্লাটার ও সিলভান অ্যাঙ্গলারকে পরবর্তী সময়ে অ্যান্ড্রয়িড অ্যাপ তৈরির জন্য নিয়োগ দেয়া হয়। ২০১৩ সালে অ্যান্ড্রয়িড অ্যাপ উন্মুক্ত করা হয়। ওই বছর স্নোডেন মার্কিন গোয়েন্দা তথ্য ফাঁস করার পর থ্রিমার জনপ্রিয়তা বাড়তে থাকে। ২০১৪ সালের ফেব্রুয়ারিতে ফেসবুক যখন হোয়াটসঅ্যাপকে কিনে নেয়, তারপর এক দিনেই থ্রিমার ব্যবহারকারী দুই লাখ বেড়ে যায়। এর মধ্যে ৮০ ভাগ জার্মানির। ২০১৪ সালে এর নাম করা হয় থ্রিমা জিএমবিএইচ।

এনক্রিপশন : তথ্য বিনিময়ে তথ্যের গোপনীয়তা নিশ্চিত করতে কোডিং ব্যবহার করার প্রক্রিয়াই হলো এনক্রিপশন। ডিজিটাল যোগাযোগের ক্ষেত্রে থার্ডপার্টি কেউ যেন তথ্য বিনিময়ের সময় অ্যাক্সেস পেলেও তথ্য উদ্ধার না করতে পারে, তার জন্যই এনক্রিপশন ব্যবহার করা হয়। এনক্রিপটেড তথ্য শুধু সুনির্দিষ্ট কোডের মাধ্যমে উদ্ধার করা যায়। ক্রিপ্টোগ্রাফির মূল অস্ত্র হলো একটি ক্রিপ্টোগ্রাফিক অ্যালগরিদম বা সাইফার, যা দিয়ে ডাটা এনক্রিপ্ট করা হয় বা এনক্রিপটেড ডাটা ডিক্রিপ্ট করা হয়। এটা মূলত একটি ম্যাথমেটিক্যাল ফাংশন। এই অ্যালগরিদম কাজ করে একটি কী'র সাথে। এই কী হতে পারে একটি শব্দ, সংখ্যা বা শব্দগুচ্ছ। একই প্লেইন টেক্সট বিভিন্ন কী'র সাহায্যে বিভিন্ন সাইফার টেক্সটে রূপান্তরিত হবে।

এনক্রিপটেড ডাটার নিরাপত্তা নির্ভর করে দুটি জিনিসের ওপর।

- ক্রিপ্টোগ্রাফিক অ্যালগরিদম শক্তি।
- কী'র নিরাপত্তা।

প্রথাগতভাবে একই কী'র মাধ্যমেই এনক্রিপশন এবং ডিক্রিপশন দুটিই করা হয়। কী'র ধরনের ওপর ভিত্তি করে এনক্রিপশনকে আমরা দুই ভাগে ভাগ করতে পারি। ০১. সিমেট্রিক এনক্রিপশন। ০২. অ্যাসিমেট্রিক এনক্রিপশন।

সিমেট্রিক এনক্রিপশন : সিমেট্যিক এনক্রিপশনে যাদের মধ্যে তথ্যের বিনিময় হয়, সেই দুই পক্ষ একই কী ব্যবহার করে থাকে। এ ক্ষেত্রে যে কী দিয়ে এনক্রিপশন করা হয়, সেই কী দিয়েই প্রাপক ডিক্রিপট করে থাকে প্রাপ্ত মেসেজকে। যেহেতু এনক্রিপশন ও ডিক্রিপশন একই কী দিয়ে হচ্ছে, তাই এই প্রক্রিয়াকে সিমেট্রিক এনক্রিপশন বলা হয়।

অ্যাসিমেট্রিক এনক্রিপশন : সিমেট্রিক এনক্রিপশনের সমস্যা হলো প্রাপক ও প্রেরকের একই কী ব্যবহার করতে হয়। কিন্তু বাস্তব জীবনে প্রাপক ও প্রেরকের মধ্যে এই কী বিনিময় খুবই ঝামেলার। এ ছাড়া এই বিনিময়ের সময় কী'র নিরাপত্তা বা গোপনীয়তাই ভঙ্গ হতে পারে। তাই বিজ্ঞানীরা এমন এক এনক্রিপশন পদ্ধতি বের করেছেন, যাতে প্রাপক ও প্রেরক ভিন্ন ভিন্ন কী ব্যবহার করলেও তাদের মধ্যে সঠিকভাবে তথ্যের বিনিময় হতে পারে।

অ্যাসিমেট্রিক এনক্রিপশনে প্রাপক ও প্রেরক মূলত এক জোড়া করে কী ব্যবহার করেন। এর মধ্যে একটি পাবলিক কী ও অপরটি প্রাইভেট কী। পাবলিক কী সবাইকে জানিয়ে দেয়া হয় আর প্রাইভেট কী একান্তই গোপন থাকে। শুধু যার প্রাইভেট কী সে-ই ওই কী জানে।

তথ্য বিনিময়ের সময় প্রথমে প্রেরক প্রাপকের পাবলিক কী সংগ্রহ করে। তারপর সে মূল মেসেজটি প্রাপকের পাবলিক কী দিয়ে এনক্রিপ্ট করে থাকে। তারপর প্রেরক সেই এনক্রিপটেড মেসেজটি প্রাপকের কাছে পাঠায়। এখন এই কমিউনিকেশনের সময় কোনো ব্যক্তি বা প্রতিষ্ঠান যদি এই এনক্রিপটেড মেসেজটি পায়, তবে সে এই এনক্রিপটেড মেসেজ থেকে মূল মেসেজটি উদ্ধার করতে পারবে না। কারণ, একমাত্র যার পাবলিক কী দিয়ে এই মেসেজটি এনক্রিপ্ট করা হয়েছে, তার প্রাইভেট কী দিয়েই তা ডিক্রিপ্ট করা যাবে। সুতরাং দেখা যাচ্ছে, যদিও একজন জঙ্গি বাংলাদেশের ইন্টারনেট সংযোগ ব্যবহার করে তার মেসেজ পাঠায় এবং সেই মেসেজ যদি এনক্রিপ্ট করা থাকে তাহলে বাংলাদেশ সরকার যদি সেই মেসেজ ইন্টারসেপ্টও করে তারপরও সেই মেসেজের মর্মোদ্ধার করতে পারবে না। তাই দেখা যায় জঙ্গিরা যেসব মেসেজিং সফটওয়্যার বা অ্যাপ এনক্রিপশন ব্যবহার করে, সে ধরনের সফটওয়্যার বা অ্যাপ তাদের কমিউনিকেশনের জন্য ব্যবহার করে থাকে।

এনক্রিপশন ব্যবহারের জন্য অনেক দেশের সরকারই অনেক ধরনের অ্যাপ তাদের দেশে নিষিদ্ধ করেছে। যেমন– ভারতে ব্ল্যাকবেরি নিষিদ্ধ করা হয়েছিল। সম্প্রতি ওরল্যান্ডো শুটআউটের পর সেই সন্ত্রাসীর আইফোনের এনক্রিপশন ব্রেক করার জন্য আইফোনের মালিক প্রতিষ্ঠান অ্যাপলের কাছে অনুরোধ করেছিল সেই দেশের আইন প্রয়োগকারী সংস্থা এফবিআই। কিন্তু এতে অন্য ব্যবহারকারীর নিরাপত্তা ভঙ্গ হতে পারে, সেই যুক্তিতে তার এফবিআইয়ের সেই আবেদন নাকচ করে দেয়।

সুতরাং বোঝা যাচ্ছে, সামনের দিনে জঙ্গি বা সন্ত্রাসীদের মাধ্যমে এই ধরনের সিকিউর অ্যাপের ব্যবহার যেমন বাড়বে, সেই সাথে সরকারের এই ধরনের সক্ষমতা বাড়ানোর বিষয়টা জড়িত। আবার একই সাথে সরকার যদি সব ধরনের এনক্রিপশন ভাঙতে পারে, তবে সাধারণ জনগণের প্রাইভেসি বা গোপনীয়তা ভঙ্গ হতে পারে বলে অনেকের মধ্যে এ নিয়ে উদ্বেগও আছে কজ

ফিডব্যাক : jabedmorshed@yahoo.com