কমিউনিকেশন সিস্টেমস
ও নেটওয়ার্কিং

1

কে. এম. শরীয়াত উল্লাহ

শিক্ষার্থী, ইলেকট্রিক্যাল এন্ড ইলেকট্রনিক ইঞ্জিনিয়ারিং বিভাগ,
শাহজালাল বিজ্ঞান ও প্রযুক্তি বিশ্ববিদ্যালয়, সিলেট।

কমিউনিকেশন কী?

সে বহুকাল আগের কথা। মানুষ পায়রার মাধ্যমে এক জায়গা থেকে অন্য জায়গায় খবরের আদান-প্রদান করত। এমনকি রাজ দরবারের নানা গোপনীয় তথ্যও পায়রার পায়ে বেধে দেওয়া হতো। খবরটি পায়রার পায়ে বেধে দেওয়ার পর একে ছেড়ে দেওয়া হতো। যার কাছে খবরটি পৌঁছানোর দরকার পায়রাটি ঠিকঠিক তার কাছে পৌঁছে যেত। এইযে একটি তথ্য [চিঠি] একটি নির্দিষ্ট চ্যানেলের মাধ্যমে [পায়রা] এক স্থান থেকে অন্য স্থানে পৌঁছে দেওয়ার পদ্ধতি, তাকে বলা হয় কমিউনিকেশন।

সঙ্গা ২.১ যে পদ্ধতিতে আমরা উপাত্ত বা তথ্যকে এক জায়গা থেকে আরেক জায়গায় বা এক ডিভাইস থেকে আরেক ডিভাইসে একটি নির্দিষ্ট চ্যানেলের মাধ্যমে স্থানান্তরিত করে সেই তথ্য সংগ্রহ করে ব্যবহার করতে পারি তাকে বলা হয় কমিউনিকেশন।

খেয়াল রাখতে হবে, একজন প্রেরক, একজন প্রাপক ও একটি নির্দিষ্ট চ্যানেল না থাকলে কমিউনিকেশন হওয়া সম্ভব না। তাছাড়া ধরুন পায়রাটি চিঠি নিয়ে পৌঁছালো। কিন্তু বৃষ্টির কারণে চিঠি এমনভাবে ভিজে গেছে যে চিঠির মধ্যে থাকা খবর আর পড়া যাচ্ছে না, তাহলে এই কমিউনিকেশনে প্রেরক, প্রাপক ও নির্দিষ্ট চ্যানেল থাকা সত্ত্বেও কমিউনিকেশনকে এখানে সাকসেসফুল বলা যায় না। তাই কমিউনিকেশনকে সফল তখনই বলা হবে যখন প্রেরক থেকে প্রাপকের কাছে নির্দিষ্ট চ্যানেল ব্যবহার করে পাঠানো তথ্যগুলো প্রাপক পুনরুদ্ধার করতে পারে।

তবে চিঠি এভাবে পায়রার মাধ্যমে পাঠানোর আরেকটা বড় সমস্যা আছে। ধরুন যে আপনি খুবই গোপন একটি খবর অন্য কাউকে পাঠাতে চাচ্ছেন এই পায়রার মধ্য দিয়ে। পায়রা উড়ে উড়ে যাচ্ছে আপনার পাঠানো তথ্য নিয়ে। মাঝ পথে আপনার বিপক্ষ দলের লোকেরা করল কি পায়রাটাকে তীর বিদ্ধ করল। পায়রার পা থেকে গোপন খবরটি নিয়ে জেনে গেল যে আপনাদের মাঝে কী কী চলছে। এটি কিন্তু আপনার জন্য বেশ ভয়াবহ একটা অবস্থা ডেকে আনতে পারে। আপনার বিপক্ষ দলের লোকেরা যাতে আপনার পাঠানো এই গোপন সংকেত পড়তে না পারে এরজন্য কী করা যায় বলুন তো?

একটা কাজ করা যায় তীর থেকে বাঁচতে সৈন্যরা যেমন লোহার তৈরি বর্ম পরিধান করে, তেমনি পায়রাকেও লোহার বর্ম পড়ানো হোক, তীর বিদ্ধ হবে না আর। তবে হ্যাঁ! আপনারাও বুঝতে পারছেন এই আইডিয়াটা একটা বোকামি! পায়রা এত ভারী লোহার বর্ম নিয়ে উড়তে পারবে না। চিঠিও পৌঁছাতে পারবে না। ফলে কমিউনিকেশন সফল হবে না। তাই কী করা উচিত এখন? অন্য আরেকটি উপায় বের করা উচিত।

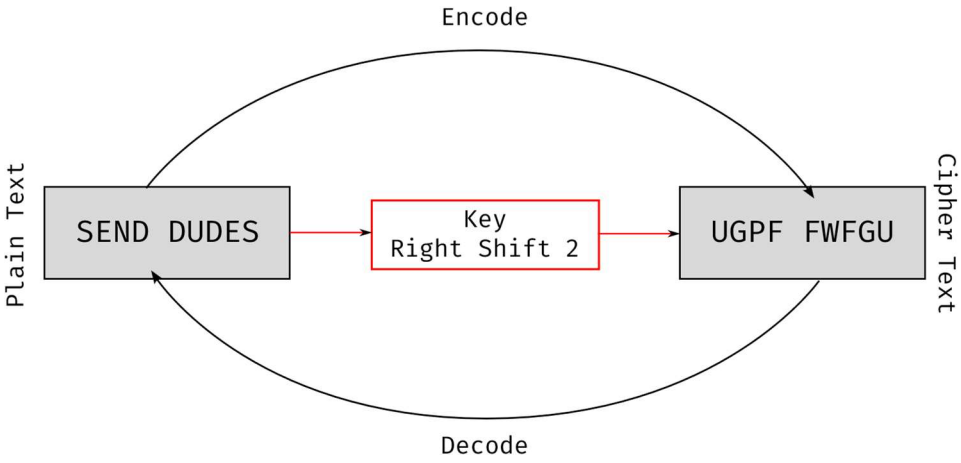
এমনই একটি সুন্দর উপায় বের করেছিলেন রোমান শাসক জুলিয়াস সিজার [100 BC – 44 BC]। তার আইডিয়াটি এতোটাই জোস ছিল যে আজও আমাদের কম্পিউটার প্রকৌশলে বা ইলেকট্রনিক্স প্রকৌশলে তার পদ্ধতির নানা প্রয়োগ রয়ে গিয়েছে। তিনি একটি কোড আবিষ্কার করেছিলেন। একে তার নামে আমরা নাম দিয়েছি সিজার কোড। সিজার কোড কী তা একটু বুঝে নেই।

ধরুন আপনার কাছে একটি কাগজে লেখা আছে SEND DUDES. এক্ষেত্রে সিজার যা করলেন তা হচ্ছে তিনি একে লিখলেন UGPF FWFGU. অর্থাৎ, মূল চিঠিতে যেই ম্যাসেজটি থাকে তার প্রতিটা অক্ষরকে দুইঘরের পরের অক্ষর দিয়ে প্রতিস্থাপন

করে দিয়েছি। তাই S হয়ে গেছে U। E হয়ে গেছে G। N হয়ে গেছে P। এভাবে ... তো এবার যদি এই চিঠি বিপক্ষ দলের লোকের হাতে পড়েও সে কনফিউজড উংগা-বুংগা অনুভব করবে। ফলে শত্রুর হাতে আমার ম্যাসেজ থাকবে না। অন্যদিকে কোনো না কোনোভাবে আমরা আমাদের প্রত্যাশিত প্রাপকের কাছে জানিয়ে দিব যে আমি দুইঘর 'শিফট' করেছি প্রতিটি অক্ষরকে। তাহলে প্রাপক শুধুই আমার পাঠানো হাবিজাবি লেখাটাকে দুইঘর পিছনে নিলেই SEND DUDES মূল ম্যাসেজটি পেয়ে যাবে। এই দুইঘর ডানে শিফট করার মাধ্যমে ম্যাসেজ গোপন করার পদ্ধতিকে Right Shift 2 Ceaser Cipher Algorithm বলে।

এইযে আমি আমার মূল ম্যাসেজকে গোপন করে ফেললাম এই প্রক্রিয়ার নাম হলো এনক্রিপশন করা। এখানে যেহেতু প্রেরক ও প্রাপক ছাড়া অন্য কেউ আমার ম্যাসেজ দেখতে পারবে না, তাই একে বলা হয় End to End Encryption।

মূল যে টেক্সটটি আমরা পাঠাতে চাচ্ছিলাম তাকে বলা হয় প্লেইন টেক্সট। এখানে SEND DUDES হলো আমাদের প্লেইন টেক্সট। সিজার কোড করে যেই গোপন ম্যাসেজটি আমরা তৈরি করেছি তাকে বলা হয় সাইফার টেক্সট। এখানে UGPF FWFGU হলো আমাদের সাইফার টেক্সট। প্রেরক প্রাপককে যেভাবে বুঝায় যে কতঘর শিফট করলে আবার মূল ম্যাসেজে ফেরত আসা যাবে তাকে বলা হয় Key বা চাবি। প্লেইন টেক্সটকে সাইফার টেক্সটে রূপান্তর করে ফেলাকে বলা হয় Encoding আর সাইফার টেক্সটকে আবার প্লেইন টেক্সটে রূপান্তর করে ফেলাকে বলা হয় Decoding।



চিত্র ২.১ সিজার সাইফার কোডের সাহায্যে একটি ম্যাসেজকে এনক্রিপ্ট করার প্রক্রিয়া।

বর্তমানে ধরুন আপনি ফোনে কারো সাথে কথা বলছেন। তো আপনি হচ্ছে তথ্য প্রেরক। অপরপাশে আরেকজন থাকবে যে আপনার পাঠানো অডিও শুনবে। সে হচ্ছে প্রাপক। এখানে মাঝের ফোন হচ্ছে চ্যানেল। এখানেও একটি এনক্রিপশন অ্যালগরিদম ব্যবহার করে আপনার পাঠানো অডিও যাতে মাঝে দিয়ে অন্য কেউ তার ফোনে না শুনে ফেলতে পারে তা নিশ্চিত করা হয়। কোনো হ্যাকার যদি কোনোভাবে এই এনক্রিপশন ভেঙ্গে ফেলতে পারে [অর্থাৎ এনক্রিপশনের চাবিটি কি এটি যদি হ্যাকার জেনে যায়] তাহলে সেও আপনার আর প্রাপকের মাঝের অডিও শুনে ফেলবে। এভাবে প্রেরক ও প্রাপকের মাঝের তথ্য গোপনে শুনে ফেলাকে Eavesdropping [ইভসড্রপিং] বলে। এটি আইনত দণ্ডনীয় অপরাধ।