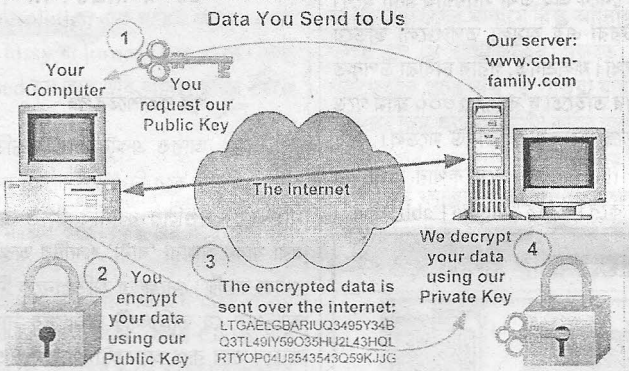
একটি তালার দুটি চাবি

গৌতমকুমার পাল, অধ্যাপক, কম্পিউটার সায়েন্স এন্ড ইঞ্জিনিয়ারিং বিভাগ, যাদবপুর বিশ্ববিদ্যালয়

কথাটা শুনলে মনে হবে এ আর এমন কি! একটি তালার শুধু দুটি কেন, তিনটি, চারটি, দশটি – যতগুলো খুশী ততগুলো চাবি বানানো যেতে পারে। কিন্তু আমি বলতে চাইছি দুটো আলাদা রকমের চাবির কথা। মানে সাধারণতঃ একটি তালার সব চাবিগুলো হুবহু একই রকমের দেখতে হয় এবং যেকোনো একটি চাবি দিয়ে তালা বন্ধ করা ও খোলা দুটি কাজই করা যায়। এদিকে দুটি আলাদা রকমের চাবি মানে তাদের দেখতে যেমন আলাদা হবে, তেমনই একটি দিয়ে শুধু তালা বন্ধের কাজ করা যাবে এবং অন্যটি দিয়ে শুধু খোলা যাবে। কোনও একটি দিয়ে দুটি কাজই হবে এমন নয়।



খুব বোকা-বোকা লাগছে ব্যাপারটা, তাই না? তোমরা বলবে এই ধরনের তালা-চাবির উপযোগিতা কী? ধরা যাক, তুমি একটি গোয়েন্দা সংস্থার অধিকর্তা। তোমার দপ্তরে একই রকমের প্রচুর বাক্স রয়েছে। সব বাক্সগুলোর জন্য মোট দু'রকমের চাবি আছে। তালা দেওয়ার এক একটা চাবি তুমি এক একজন ইনফর্মারকে দিয়ে রেখেছ, আর খোলার কমন চাবিটি তোমার কাছে রয়েছে। এরকম ব্যবস্থা কেন করবে? ধর, তুমি চাইছ যে ইনফর্মাররা নিজেদের সংগৃহীত তথ্য, সাক্ষ্যপ্রমাণমূলক জিনিসপত্র ইত্যাদি এক একটা বাক্সে রাখুক (হতে পারে তোমার অনুপস্থিতিতে) কিন্তু একজন ইনফর্মারের জিনিস যাতে অন্যজন না দেখতে পায় (অনেক সংস্থায় পুরনো অপরাধীদেরই ইনফর্মার হিসেবে নিযুক্ত করা হয়)। সেক্ষেত্রে উপরোক্ত পদ্ধতিটি তুমি যা চাইছ তা অর্জনের অন্যতম উপায়। তুমি মাঝে মাঝে তোমার দপ্তরে এসে তোমার চাবিটি দিয়ে তালাগুলো খুলে জিনিসগুলো নিয়ে নিতে পারো বা অন্যত্র দিতে পারো বিশ্লেষণের জন্য।

উপরের গোয়েন্দা সংস্থার উদাহরণটি কাল্পনিক। কিন্তু গোপন তথ্য আদান-প্রদানের জন্য অনুরূপ ব্যবস্থা নেওয়া হয় ই-কমার্স *অ্যাপ্লিকেশনস্-এ* বা সিকিউর শেল (এস্ এস্ এইচ্)-এর *কী অথেন্টিকেশন প্রোটোকল-এ*, অথবা *ডিজিটাল সিগনেচার স্কিম-এ*। টেকনিক্যাল ভাষায় ব্যাপারটাকে বলা হয় *পাবলিক কী ক্রিপটোগ্রাফি*। *ক্রিপটোগ্রাফিতে* কিছু তথ্য *এনক্রিপ্ট* (অর্থাৎ এনকোড) বা *ডিক্রিপ্ট* (অর্থাৎ ডিকোড)করার জন্য একটি বিশেষ সংখ্যা বা শব্দ লাগে (অনেকটা *পাস্ওয়ার্ড*-এর মতো),

৫ পাতায়

তালার দুটি চাবি

প্রথম পাতারপর

যাকে বলা হয় 'কী' বা চাবি। সাধারনত, এনক্রিপ্ট বা ডিক্রিপ্ট একই 'কী' দিয়ে করা হয় অর্থাৎ তালা বন্ধ করার এবং খোলার চাবিটি একই ছাঁচের। কিন্তু পাবলিক কী ক্রিপটোগ্রাফিতে এনক্রিপ্ট এবং ডিক্রিপ্ট করার 'কী' আলাদা, তাদের যথাক্রমে বলে *পাবলিক কী* এবং *প্রাইভেট কী*। ধরা যাক তুমি চাইছ অন্যেরা তোমাকে এনক্রিপ্টে ড তথ্য পাঠাক। সেক্ষেত্রে তুমি অঙ্ক কষে একটি *পাবলিক কী* এবং একটি *প্রাইভেট কী* নির্ণয় করবে। তারপর *পাবলিক কী* টি তুমি ঢাক পিটিয়ে সবাইকে জানিয়ে দাও (ঢাক পেটানোর অন্যতম উপায় তোমার ওয়েবসাইটে তুলে দেওয়া)। এবার যে কেউ তোমাকে এনক্রিপ্টে ড তথ্য পাঠাতে পারে, যা অন্য কারো হাতে গেলেও কেউ ডিক্রিপ্ট করতে পারবে না, কারন ডিক্রিপ্ট করার *প্রাইভেট কী* টি শুধু তোমার কাছেই রয়েছে।

তুমি বলবে বাহ বেশ ভালো ব্যাপার। এতে সুরক্ষাও সাধারন ক্রিপটোগ্রাফির চেয়ে বেশী, সেটাও সহজেই বোধগম্য। কিন্তু যে প্রশ্নটা তোমার মনে জাগছে, সেটা হল এভাবে তো একমুখী যোগাযোগ হল শুধু। অর্থাৎ তুমি কেবল তথ্য রিসিভ করলে। কিন্তু যদি সেন্ড করতে চাও তাহলে? খুব সোজা! যাকে পাঠাতে চাও, তার *পাবলিক কী* দিয়ে এনক্রিপ্ট করে পাঠাও, সে তার নিজের *প্রাইভেট কী* দিয়ে সেটা ডিক্রিপ্ট করে নেবে। যেহেতু সে নিজের *পাবলিক কী* এবং *প্রাইভেট কী* নিজে পছন্দ করেছে, সেটা বাস্তবে তোমার কী-গুলোর চেয়ে আলাদাই হবে।

পাবলিক কী ক্রিপটোগ্রাফির অনেকগুলি পদ্ধতি (*অ্যালগরিদম্*) রয়েছে। তার মধ্যে সবচেয়ে জনপ্রিয় হল 'আরএসএ', যার নামকরণ হয়েছে তিন আবিষ্কর্তা *রন রিভেস্ট, আডি শমির* এবং *লেন অ্যাডলম্যান*-এর পদবীর আদ্যক্ষর অনুসারে। ১৯৭৭ সালে 'এমআইটি' (*ম্যাসাচুসেটস্ ইনস্টিটিউট অফ টেকনোলজি*)-তে গবেষণারত অবস্থায় তাঁরা এই পদ্ধতিটি আবিস্কার করেন এবং এই আবিস্কারের সুদূরপ্রসারী প্রয়োগের স্বীকৃতিস্বরূপ ২০০২ *সালে টিউরিং অ্যাওয়ার্ড* (যাকে কম্পিউটার সায়েন্সের *নোবেল* বলা হয়) লাভ করেন।

শুনতে আশ্চর্য লাগলেও একথা সত্যি যে 'আরএসএ' এর সুরক্ষা নির্ভর করছে যৌগিক সংখ্যাকে উৎপাদকে বিশ্লেষণের মতো আপাতসহজ সমস্যার কাঠিন্যের (*কমপ্লেক্সিটি*) উপর। আপাতজটিল জিনিসের মধ্য থেকে সহজ সত্যের উদঘাটন অথবা আপাত সহজ জিনিসের মধ্যে লুকোনো গভীর তাৎপর্যের পরিস্ফুটন - - বিজ্ঞানের সৌন্দর্য বোধহয় এখানেই।