ডিজিটাল স্বাক্ষর
কী, কেন এবং কিভাবে

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

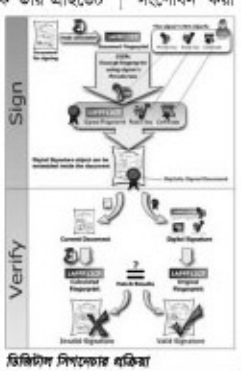
সাধারণত ব্যাংকে কোনো চেক জমা দিলে ব্যাংকের ভারপ্রাপ্ত কর্মকর্তা চেকদাতার স্বাক্ষরটি খুব ভালোভাবে পরীক্ষা করে তবেই প্রাপককে টাকা দেন। আসলে এ পরীক্ষার মাধ্যমে ব্যাংক কর্মকর্তা নিশ্চিত হতে চান, চেকে কোনো ধরনের জালিয়াতি করা হয়নি। এভাবে আমাদের হাতের দেয়া স্বাক্ষর যুগ যুগ ধরে আমাদের স্বাতন্ত্র্য তুলে ধরেছে।

স্বাক্ষরের মূল ব্যাপারটা কী? এটা এমন একটা ব্যাপার, যা শুধু স্বাক্ষরদাতাই করতে পারেন, আর সবাই সেটাকে যাচাই করতে পারেন।

ইলেকট্রনিক মাধ্যমে কিভাবে স্বাক্ষর করা সম্ভব? স্বাক্ষরের মূল নীতিটা চিন্তা করলেই এর জবাব বেরিয়ে আসবে। স্বাক্ষরের মূল নীতি হলো–যিনি স্বাক্ষর দিচ্ছেন, তিনিই শুধু স্বাক্ষরটা দিতে পারবেন, কিন্তু অন্য সবাই সেটা যাচাই করতে পারবেন। ডিজিটাল স্বাক্ষরের মূল বিষয়টি নিহিত আছে পাবলিক কী-ক্রিপ্টোগ্রাফিতে।

পাবলিক কী-ক্রিপ্টোগ্রাফিতে একজোড়া কী বা চাবি থাকে, যার একটা সবাই জানে (পাবলিক কী), আরেকটা শুধু চাবির মালিক জানে (প্রাইভেট কী)। একটা চাবি দিয়ে তথ্যকে গুপ্ত করে ফেললে অন্য চাবি দিয়ে সেটাকে প্রকাশ করা যায়। তথ্যগোপনবিদ্যায় এই কায়দা ব্যবহার করা হয় কাউকে গোপন বার্তা পাঠাতে। বার্তাটাকে পাবলিক কী দিয়ে গোপন করলে শুধু যার কাছে প্রাইভেট কী আছে, সেই শুধু প্রাইভেট কী দিয়ে বার্তাটার মর্মোদ্ধার করতে পারবেন।

এই কায়দাটাকেই কিন্তু উল্টো করে ব্যবহার করা চলে। স্বাক্ষর করার ক্ষেত্রে যদি মূল বার্তা বা তার সারাংশকে বার্তা প্রেরক তার প্রাইভেট কী দিয়ে স্বাক্ষর করে, তাহলে পাবলিক কী দিয়ে সেই গোপন সারাংশের মর্মোদ্ধার যেকেউ করে যাচাই করতে পারবেন, আসলেই এটা বার্তা প্রেরকের স্বাক্ষরিত কি না। পাবলিক কী দিয়ে সেসব বার্তাই খোলা যাবে, যা প্রাইভেট কি দিয়ে বন্ধ করা হয়েছে। আর যেহেতু প্রাইভেট কী শুধু বার্তা প্রেরকেরই জানা, অন্য সবার অজানা, তাই এই ক্ষেত্রে নিশ্চিত হওয়া যাবে, বার্তা প্রেরকই এটা পাঠিয়েছে।



ডিজিটাল সিগনেচার প্রক্রিয়া

পুরো পদ্ধতিটা দাঁড়ায় এমন– বার্তা পাঠানোর সময় বার্তার সাথে সাথে স্বাক্ষরিত সারাংশ পাঠানো হয়। সারাংশ নির্মাণের পদ্ধতিটি হলো হ্যাশিং, এর মাধ্যমে যেকোনো আকারের বার্তাকেই নির্দিষ্ট আকারের সারাংশে পরিণত করা চলে। এরপর বার্তা প্রেরক সেই সারাংশকে প্রাইভেট কী দিয়ে লুকিয়ে রাখেন।

বার্তা যে পাবেন বা যে বার্তাটাকে যাচাই করতে চাইবেন, তার কাজ হবে প্রথমে বার্তার সারাংশ বানানো ওই একই হ্যাশিং পদ্ধতিতে। এর পাশাপাশি প্রেরকের পাবলিক কী দিয়ে লুকিয়ে রাখা সারাংশটাকেও খুলে নিতে হবে। এরপর দেখতে হবে লুকিয়ে রাখা সারাংশটা গ্রাপক নিজে যে সারাংশ হিসাব করে পেয়েছেন, তার সাথে মিলে কি না।

আধুনিক ইন্টারনেটে বার্তার উৎস যাচাই করার জন্য এরকম ডিজিটাল স্বাক্ষর অনেক ক্ষেত্রেই ব্যবহার করা হচ্ছে। ব্যাংকের ওয়েবসাইট থেকে শুরু করে ই-মেইলেও এর প্রয়োগ আছে। বলা হয়, এই স্বাক্ষর ব্যবস্থা না থাকলে ই-কমার্স বা ইন্টারনেট ব্যাংকিং আদৌ সম্ভব হতো না।

আমাদের দেশে ২০০২ সালে তথ্য ও যোগাযোগ প্রযুক্তি আইনে ইলেকট্রনিক সই পদ্ধতি অন্তর্ভুক্ত করা হয়। ২০০২ সালের এ আইনটি ২০০৬ সালের অক্টোবরে সংসদে পাস হয়। সেই আইনে বলা হয়, আইনটি পাস হওয়ার ৯০ দিনের মধ্যে ইলেকট্রনিক সই প্রবর্তনের জন্য প্রয়োজনীয় কর্তৃপক্ষ গঠন করতে হবে। কিন্তু আইনটি পাস হওয়ার ২০ দিন পরই সেই সংসদের মেয়াদ শেষ হয়ে যায়। এরপর আবার অধ্যাদেশ জারি করা হয়। বর্তমান সরকার ক্ষমতায় আসার পর সেই অধ্যাদেশটি সংশোধন করা হয়। ফলে ইলেকট্রনিক সই পদ্ধতির জন্য প্রয়োজনীয় অবকাঠামো তৈরির সুযোগ হয়। একটি সংস্থাকে ইলেকট্রনিক সনদের নিয়ন্ত্রক হিসেবে কাজ করতে হয়। বাংলাদেশ কমপিউটার কাউন্সিলের নির্বাহী পরিচালককে প্রধান করে কন্ট্রোলার অব সার্টিফাইং অথরিটি তথা সিসিএ নামে একটি সরকার নিয়ন্ত্রিত সংস্থা চালু করা হয়েছে। ইলেকট্রনিক সনদ দেয়ার জন্য কিছু অনুমোদিত প্রতিষ্ঠান থাকে। এসব প্রতিষ্ঠানকে বলা হয় সার্টিফিকেট অথরিটি তথা সিএ। এই সিএদের লাইসেন্স দেবে সিসিএ। সার্টিফিকেট অথরিটির মূল দায়িত্ব হচ্ছে তার গ্রাহকের পরিচিতি নিশ্চিত করা, তাদের প্রাইভেট ও পাবলিক চাবি তৈরিতে সাহায্য করা, প্রাইভেট চাবি গ্রাহকের কাছে পুরোপুরি হস্তান্তর করা এবং পাবলিক চাবি ডিরেক্টরিতে প্রকাশ করা। এই প্রকাশিত পাবলিক চাবি কোন কাজে ব্যবহার করা যাবে এবং গ্রাহকের প্রয়োজনীয় তথ্যসহ সিএ নিজ স্বাক্ষর দিয়ে একটি সার্টিফিকেট ওই ডিরেক্টরিতে সাজিয়ে রাখবে। যদি কখনো কোনো কারণে প্রাইভেট চাবি খোয়া যায় বা প্রাইভেট চাবি ব্যবহারের অনুপযোগী হয়ে পড়ে, তবে তা তাৎক্ষণিকভাবে সিএ-কে জানাতে হবে, যাতে সিএ তার নামে দেয়া সার্টিফিকেট বাতিল করে বাতিলের তালিকায় অন্তর্ভুক্ত করতে পারে। এতে কোনো ব্যবহারকারী ওই গ্রাহকের সার্টিফিকেট বাতিলের সময়ের পরে পাওয়া স্বাক্ষর সঠিক বলে ধরে নেবেন না, কিন্তু আগের করা স্বাক্ষর মেলাবার জন্য বাতিলের তালিকাতে খুঁজতে হবে।

২০০৯ সালে তথ্য ও যোগাযোগ প্রযুক্তি আইনের সংশোধনীর মাধ্যমে দেশে ডিজিটাল স্বাক্ষর চালুর বৈধ আইনি কাঠামো বলবৎ হয়েছে। এ আইনের আওতায় সরকার ইতোমধ্যে সার্টিফিকেট দানকারী কর্তৃপক্ষের নিয়ন্ত্রকের কার্যালয় প্রতিষ্ঠা করেছে। ২০১০ সালের এপ্রিল মাসে সার্টিফিকেটের দানকারী কর্তৃপক্ষ গঠনের প্রয়োজনীয় বিধিমালা জারি করা হয়েছে। ২০১১ সালের ১৯ জানুয়ারি সরকার কর্তৃক মেসার্স বাংলা ফোন লিমিটেড, মেসার্স কমপিউটার সার্ভিসেস লিমিটেড, মেসার্স ডাটা এজ লিমিটেড, মেসার্স দোহাটেক নিউ মিডিয়া, মেসার্স ফ্লোরা টেলিকম লিমিটেড এবং মেসার্স ম্যাংগো টেলিসার্ভিসেস লিমিটেডকে বাণিজ্যিকভাবে ডিজিটাল সনদ দানসহ সার্টিফাইং অথরিটির তথা সিএ কার্যক্রম পরিচালনার জন্য লাইসেন্স দেয়া হয়েছে।

ডিজিটাল স্বাক্ষর ঠিকমতো চালু করতে পারলে আমাদের অফিসগুলোতে আরো নিরাপদ ও বৈধভাবে ফাইল দেয়া-নেয়া সম্ভব হবে। কোনো ফাইল বা ডকুমেন্ট নিয়ে কোনো আইনি জটিলতা দেখা দিলে ডিজিটাল স্বাক্ষরের মাধ্যমে তার প্রেরক ও গ্রাহককে সহজেই শনাক্ত করা সম্ভব হবে। ফলে যেকোনো ব্যাপারে দ্রুত আইনি পদক্ষেপ নেয়া যাবে। তবে ডিজিটাল স্বাক্ষরের সবচেয়ে বড় সুবিধা হবে ই-কমার্সের ক্ষেত্রে। ডিজিটাল স্বাক্ষরের মাধ্যমে একজন ক্রেতা সহজেই একটি বৈধ সাইট ও প্রতারক সাইটের মধ্যে পার্থক্য ধরে ফেলতে পারবেন। কারণ ডিজিটাল সার্টিফিকেট শুধু প্রকৃত ই-কমার্স সাইটকেই দান করা হবে। যেকোনো আর্থিক লেনদেন হবে এই সার্টিফিকেটের মাধ্যমে। ফলে ইচ্ছা করলে আইন প্রয়োগকারী সংস্থা কোনোরূপ বেআইনি লেনদেন সহজেই শনাক্ত করতে পারবে। তাই পরিশেষে বলা যায়, আমাদের উচিৎ যত দ্রুত সম্ভব সর্বস্তরে ডিজিটাল স্বাক্ষর চালু করা।

ফিডব্যাক : jabedmorshed@yahoo.com