৬.৪ Key ম্যানেজমেন্ট, ডিজিটাল সিগনেচার ও ডিজিটাল সার্টিফিকেট

কী ম্যানেজমেন্ট কী?

ডেটা এনক্রিপ্ট এবং ডিক্রিপ্ট করার জন্য 'Key' বা চাবি ব্যবহার করা হয়। ক্রিপ্টোগ্রাফির জগতে এই চাবি বা Key হলো তথ্য সুরক্ষার মূল ভিত্তি। কিন্তু শুধুমাত্র শক্তিশালী Key তৈরি করাই যথেষ্ট নয়, এই Key গুলোকে সঠিকভাবে পরিচালনা করাও অত্যন্ত গুরুত্বপূর্ণ। এখানেই আসে Key Management বা কী ম্যানেজমেন্টের ধারণা।

Key Management হলো ক্রিপ্টোগ্রাফিক Key-গুলোকে নিরাপদে তৈরি, সংরক্ষণ, বিতরণ এবং ধ্বংস করার একটি সুনির্দিষ্ট প্রক্রিয়া। এটি একটি সম্পূর্ণ জীবনচক্র যা নিশ্চিত করে যে, Key গুলো তাদের পুরো জীবনকাল জুড়ে নিরাপদ থাকে এবং সঠিকভাবে ব্যবহৃত হয়।

কী ম্যানেজমেন্ট সিস্টেমের ধাপসমূহ

একটি কার্যকর কী ম্যানেজমেন্ট সিস্টেম বেশ কিছু গুরুত্বপূর্ণ ধাপের সমন্বয়ে গঠিত। প্রতিটি ধাপ Key-এর নিরাপত্তা নিশ্চিত করতে গুরুত্বপূর্ণ ভূমিকা পালন করে। ধাপগুলো বিস্তারিতভাবে জেনে নেই:

১. **Key Generation (কী জেনারেশন বা চাবি তৈরি):** এই ধাপে নিরাপদে ও দৈবচয়ন পদ্ধতিতে নতুন Key তৈরি করা হয়। Key Generation প্রক্রিয়ায় বিশেষ অ্যালগরিদম ব্যবহার করে এমন একটি Key তৈরি করা হয় যা অনুমান করা প্রায় অসম্ভব। এই প্রক্রিয়ায় Random Number Generator ব্যবহার করা হয় যাতে Key টি সম্পূর্ণরূপে এলোমেলো এবং অনন্য হয়।

২. **Key Storage (কী স্টোরেজ বা চাবি সংরক্ষণ):** Key তৈরি হওয়ার পর এটিকে অত্যন্ত সুরক্ষিত স্থানে সংরক্ষণ করা অপরিহার্য। এই ধাপে Key গুলোকে এমন স্থানে রাখা হয় যেখানে অননুমোদিত কেউ প্রবেশ করতে না পারে। Key Storage-এর জন্য বিশেষ হার্ডওয়্যার বা সফটওয়্যার ভল্ট ব্যবহার করা হয় যেগুলো অতিরিক্ত সুরক্ষা স্তর প্রদান করে।

৩. **Key Distribution (কী ডিস্ট্রিবিউশন বা চাবি বিতরণ):** এই পর্যায়ে নিরাপদে সঠিক প্রাপকের কাছে Key পৌঁছে দেয়া হয়। Key Distribution একটি অত্যন্ত সংবেদনশীল প্রক্রিয়া কারণ এই সময়ে Key সবচেয়ে ঝুঁকির মধ্যে থাকে। যদি Key বিতরণের সময় কোনো তৃতীয় পক্ষ এটি বাধা দিয়ে পায়, তাহলে পুরো যোগাযোগ ব্যবস্থা বিপন্ন হয়ে পড়ে। এজন্য Key বিতরণের জন্য বিশেষ সুরক্ষিত চ্যানেল ব্যবহার করা হয়। কখনো কখনো Key কে ছোট ছোট অংশে ভেঙে আলাদা আলাদা পথে পাঠানো হয়, যাতে পুরো Key একসাথে কারো হাতে না পড়ে।

৪. **Key Usage (কী ইউজেজ বা চাবি ব্যবহার):** এই ধাপে Key ব্যবহারের ক্ষেত্রে নির্দিষ্ট নীতি অনুসরণ করা হয়। প্রতিটি Key-এর একটি নির্দিষ্ট উদ্দেশ্য এবং ব্যবহারের সীমা থাকে। উদাহরণস্বরূপ, কোনো Key শুধুমাত্র তথ্য এনক্রিপ্ট করার জন্য ব্যবহার করা যাবে, আবার অন্য Key শুধু ডিক্রিপ্ট করার জন্য। Key Usage নীতিমালায় আরও থাকে - কতবার একটি Key ব্যবহার করা যাবে, কতদিন পর্যন্ত এটি বৈধ থাকবে, এবং কোন কোন ক্ষেত্রে এটি ব্যবহার করা যাবে। এই নীতিমালা মেনে চলা Key-এর দীর্ঘমেয়াদী নিরাপত্তা নিশ্চিত করে।

৫. **Key Destruction (কী ডিস্ট্রাকশন বা চাবি ধ্বংস):** সবশেষে মেয়াদ শেষ হয়ে গেলে বা প্রয়োজন ফুরালে Key গুলো স্থায়ীভাবে ধ্বংস করে ফেলা হয়। Key Destruction একটি অত্যন্ত জরুরি পদক্ষেপ। পুরনো বা অব্যবহৃত

Key যদি সঠিকভাবে ধ্বংস না করা হয়, তাহলে সেগুলো পরবর্তীতে নিরাপত্তা ঝুঁকি তৈরি করতে পারে। Key ধ্বংস করার অর্থ শুধু ফাইল ডিলিট করা নয়, বরং এমনভাবে মুছে ফেলা যাতে কোনো প্রযুক্তি ব্যবহার করেও সেই Key পুনরুদ্ধার করা সম্ভব না হয়। এজন্য বিশেষ Cryptographic Erase পদ্ধতি ব্যবহার করা হয়।

ডিজিটাল সিগনেচার কী?

আমরা সবাই কাগজে স্বাক্ষর করতে অভ্যস্ত। আমাদের স্বাক্ষর প্রমাণ করে যে, ওই ডকুমেন্টটি আমরাই তৈরি করেছি এবং এতে আমাদের সম্মতি আছে। যখন আপনি কোনো চেক সই করেন, চুক্তিপত্রে স্বাক্ষর করেন, বা কোনো দলিল সত্যায়ন করেন - আপনার স্বাক্ষর আপনার পরিচয় এবং সম্মতির প্রমাণ বহন করে।

ডিজিটাল দুনিয়ায় এই কাজটি করে ডিজিটাল সিগনেচার। এটি প্রেরকের পরিচয় যেমন নিশ্চিত করে, পাশাপাশি তথ্যটি কেউ পরিবর্তন করেছে কিনা তাও যাচাই করা যায়। ডিজিটাল সিগনেচার হলো একটি গাণিতিক কৌশল যা ইলেকট্রনিক মেসেজ বা ডকুমেন্টের সত্যতা এবং অখণ্ডতা নিশ্চিত করে।

ডিজিটাল সিগনেচারের গুরুত্ব

ডিজিটাল সিগনেচার তিনটি প্রধান উদ্দেশ্য পূরণ করে:

১. Authentication: এটি নিশ্চিত করে যে মেসেজটি প্রকৃতপক্ষে সেই ব্যক্তির কাছ থেকে এসেছে যে পাঠিয়েছে বলে দাবি করছে।

২. Integrity: এটি নিশ্চিত করে যে মেসেজ পাঠানোর পর কেউ এতে কোনো পরিবর্তন করেনি।

৩. Non-repudiation: প্রেরক পরবর্তীতে অস্বীকার করতে পারবে না যে সে মেসেজটি পাঠায়নি।

ডিজিটাল সিগনেচার কীভাবে কাজ করে?

ডিজিটাল সিগনেচারের কার্যপ্রণালী বোঝার জন্য চলুন একটি বাস্তব পরিস্থিতি কল্পনা করি। ধরা যাক, প্রেরক একজন প্রাপককে একটি গুরুত্বপূর্ণ বার্তা পাঠাবেন। প্রেরক চান যেন প্রাপক নিশ্চিত হতে পারে যে বার্তাটি সত্যিই তার কাছ থেকে এসেছে এবং পথে কেউ এতে কোনো পরিবর্তন করেনি।

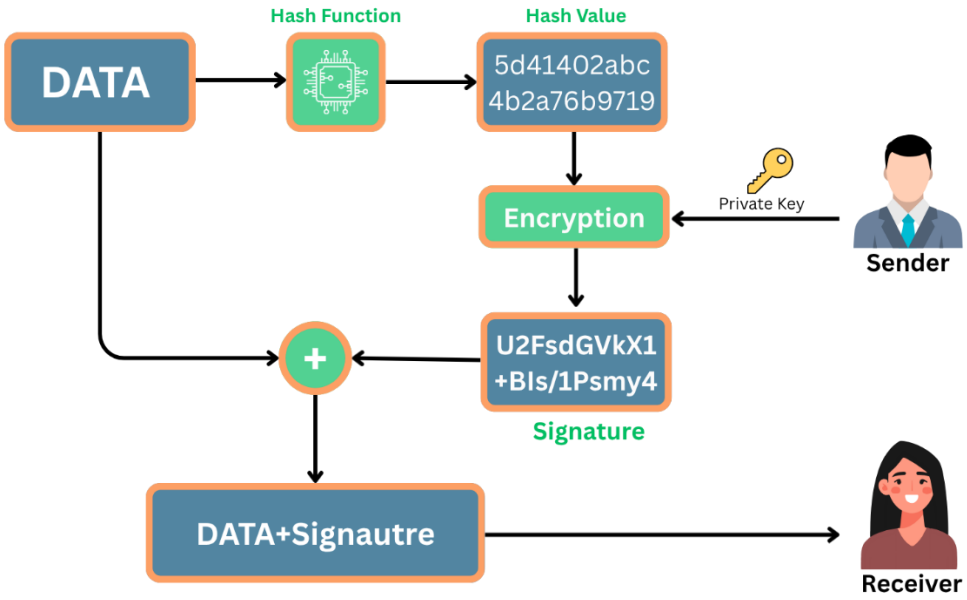
ধাপ ১ (হ্যাশ তৈরি): প্রথমে প্রেরক তার বার্তাটির একটি হ্যাশ তৈরি করেন। হ্যাশ হলো একটি বিশেষ গাণিতিক ফাংশন যা যেকোনো দৈর্ঘ্যের বার্তা থেকে একটি নির্দিষ্ট দৈর্ঘ্যের অনন্য সংখ্যা তৈরি করে। এই হ্যাশ হলো বার্তার একটি ডিজিটাল আঙুলের ছাপের মতো - প্রতিটি বার্তার জন্য অনন্য।

বার্তায় সামান্য পরিবর্তন হলেও হ্যাশ সম্পূর্ণ ভিন্ন হয়ে যায়। এই বৈশিষ্ট্যটি হ্যাশকে তথ্য যাচাইয়ের জন্য অত্যন্ত কার্যকর করে তোলে।

ধাপ ২ (হ্যাশ এনক্রিপ্ট করা): এরপর প্রেরক সেই হ্যাশটিকে তার Private Key দিয়ে এনক্রিপ্ট করেন। এই এনক্রিপ্টেড হ্যাশটিই হলো ডিজিটাল সিগনেচার। Private Key হলো প্রেরকের একটি গোপন চাবি যা শুধুমাত্র তার কাছেই আছে। অন্য কেউ এই Key-এর মালিক নয় এবং কেউ এটি জানে না।

যেহেতু শুধুমাত্র প্রেরকের কাছে Private Key আছে, তাই শুধুমাত্র সেই এই ডিজিটাল সিগনেচার তৈরি করতে পারে। এটি হাতে লেখা স্বাক্ষরের মতোই অনন্য।

ধাপ ৩ (বার্তা ও সিগনেচার পাঠানো): সবশেষে প্রেরক মূল বার্তা এবং তার সাথে এই ডিজিটাল সিগনেচারটি প্রাপকের কাছে পাঠিয়ে দেন। উভয়ই একসাথে পাঠানো হয় যাতে প্রাপক বার্তা যাচাই করতে পারে।



যাচাইকরণ প্রক্রিয়া:

প্রাপক যখন বার্তা পান, তখন তিনি নিম্নলিখিত ধাপে ডিজিটাল সিগনেচার যাচাই করেন:

১. প্রাপক প্রেরকের Public Key ব্যবহার করে ডিজিটাল সিগনেচার ডিক্রিপ্ট করেন এবং মূল হ্যাশ পান।

২. প্রাপক নিজে মূল বার্তা থেকে একটি নতুন হ্যাশ তৈরি করেন।

৩. এরপর উভয় হ্যাশ তুলনা করা হয়। যদি দুটি হ্যাশ মিলে যায়, তাহলে এটি প্রমাণ করে যে:

- বার্তাটি প্রকৃতপক্ষে সেই প্রেরকের কাছ থেকে এসেছে
- বার্তায় কোনো পরিবর্তন হয়নি

যদি হ্যাশ না মেলে, তাহলে বুঝতে হবে হয় বার্তায় কেউ পরিবর্তন করেছে, অথবা সিগনেচারটি জাল।

ডিজিটাল সার্টিফিকেট কী?

ডিজিটাল সার্টিফিকেটকে আমরা একটি ডিজিটাল পরিচয়পত্রের সাথে তুলনা করতে পারি। যেমন আমাদের জাতীয় পরিচয়পত্র বা পাসপোর্ট আমাদের পরিচয় বহন করে এবং সরকার কর্তৃক সত্যায়িত থাকে, ঠিক তেমনি ডিজিটাল সার্টিফিকেট একটি পাবলিক Key-কে নির্দিষ্ট একজন ব্যক্তি বা প্রতিষ্ঠানের নামে সত্যায়িত করে।

আপনার জাতীয় পরিচয়পত্রে যেমন আপনার ছবি, নাম, জন্ম তারিখ এবং সরকারি সীলমোহর থাকে, তেমনি ডিজিটাল সার্টিফিকেটেও মালিকের তথ্য, পাবলিক Key এবং একটি বিশ্বস্ত কর্তৃপক্ষের সত্যায়ন থাকে।

Certificate Authority (CA) কী?

ডিজিটাল সার্টিফিকেট সত্যায়িত করার কাজটি করে একটি বিশ্বস্ত তৃতীয় পক্ষ, যাকে Certificate Authority বা CA বলা হয়। Certificate Authority হলো একটি নির্ভরযোগ্য সংস্থা যা ডিজিটাল সার্টিফিকেট জারি এবং পরিচালনা করে।

CA-এর ভূমিকা অনেকটা সরকারের পরিচয়পত্র বিভাগের মতো। সরকার যেমন আপনার পরিচয় যাচাই করে পরিচয়পত্র প্রদান করে, তেমনি CA ও ব্যক্তি বা প্রতিষ্ঠানের পরিচয় যাচাই করে ডিজিটাল সার্টিফিকেট প্রদান করে। CA-এর সত্যায়ন থাকার কারণে অন্যরা সেই সার্টিফিকেটকে বিশ্বাস করতে পারে।

ডিজিটাল সার্টিফিকেট কীভাবে কাজ করে?

ডিজিটাল সার্টিফিকেট পাওয়ার এবং ব্যবহারের প্রক্রিয়া বেশ কয়েকটি ধাপে সম্পন্ন হয়। চলুন এই ধাপগুলো বিস্তারিতভাবে জেনে নেই:

ধাপ ১ (আবেদন করা): ডিজিটাল সার্টিফিকেটের প্রয়োজন হলে কোনো ব্যক্তি বা প্রতিষ্ঠান প্রথমেই একটি Certificate Authority-এর নিকট আবেদন করে। আবেদনের সময় আবেদনকারীকে তার সম্পূর্ণ তথ্য প্রদান করতে হয় এবং তার Public Key জমা দিতে হয়।

এই আবেদনে অন্তর্ভুক্ত থাকে আবেদনকারীর নাম, ঠিকানা, সংস্থার নাম (যদি প্রতিষ্ঠানের জন্য হয়), ইমেইল এবং অন্যান্য প্রাসঙ্গিক তথ্য।

ধাপ ২ (পরিচয় যাচাই): তখন Certificate Authority আবেদনকারীর পরিচয় যাচাই করে। এই যাচাইকরণ প্রক্রিয়া অত্যন্ত কঠোর এবং বিস্তৃত। CA নিশ্চিত করে যে আবেদনকারী প্রকৃতপক্ষে যে পরিচয় দাবি করছে, সেই ব্যক্তি বা প্রতিষ্ঠান।

যাচাইকরণের জন্য CA বিভিন্ন নথি পরীক্ষা করে, ফোন বা ইমেইলে যোগাযোগ করে, এবং প্রয়োজনে সরাসরি দলিলপত্র পরীক্ষা করে। একটি ওয়েবসাইটের জন্য সার্টিফিকেট হলে, CA যাচাই করে যে আবেদনকারী সত্যিই ওই ডোমেইনের মালিক।

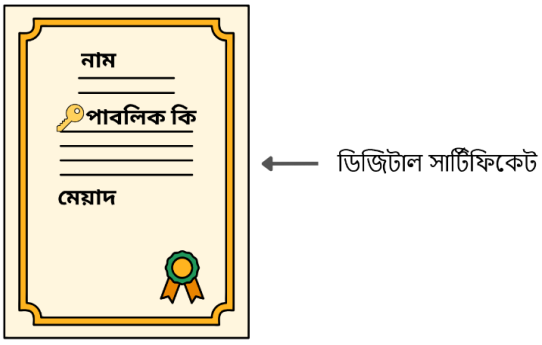
ধাপ ৩ (সার্টিফিকেট তৈরি): পরিচয় নিশ্চিত হওয়ার পর, CA একটি সার্টিফিকেট তৈরি করে। এই সার্টিফিকেটে আবেদনকারীর নাম, তার পাবলিক কী, সার্টিফিকেটের মেয়াদ ইত্যাদি তথ্য থাকে।

সার্টিফিকেটে থাকে:

- মালিকের নাম এবং তথ্য
- মালিকের Public Key
- সার্টিফিকেটের সিরিয়াল নম্বর
- সার্টিফিকেটের বৈধতার সময়কাল (কখন থেকে কখন পর্যন্ত বৈধ)
- CA-এর নাম এবং তথ্য
- ব্যবহৃত ক্রিপ্টোগ্রাফিক অ্যালগরিদম

ধাপ ৪ - ডিজিটাল সিগনেচার যুক্ত করা: সবশেষে, CA তার নিজের প্রাইভেট কী দিয়ে সার্টিফিকেটটিতে একটি ডিজিটাল সিগনেচার যুক্ত করে দেয়। এটাই প্রমাণ করে যে সার্টিফিকেটটি আসল এবং বিশ্বস্ত। CA-এর এই ডিজিটাল সিগনেচার হলো সার্টিফিকেটের সত্যতার চূড়ান্ত প্রমাণ।

যে কেউ এই সার্টিফিকেট দেখলে CA-এর Public Key ব্যবহার করে সিগনেচার যাচাই করতে পারে এবং নিশ্চিত হতে পারে যে সার্টিফিকেটটি সত্যিই ওই CA থেকে এসেছে এবং কেউ এতে পরিবর্তন করেনি।



এই সার্টিফিকেট নিশ্চিত করে যে আপনি সত্যিই সঠিক ওয়েবসাইটে আছেন এবং আপনার ও ওয়েবসাইটের মধ্যে যোগাযোগ এনক্রিপ্টেড ও নিরাপদ। এর মাধ্যমে আপনার পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য এবং অন্যান্য সংবেদনশীল তথ্য সুরক্ষিত থাকে।

এই পাঠে যে বিষয়গুলো আলোচনা করা হয়েছে:

১. কী ম্যানেজমেন্ট (Key Management) এবং এর গুরুত্ব
২. কী ম্যানেজমেন্ট সিস্টেমের ৫টি ধাপ (Generation, Storage, Distribution, Usage, Destruction)
৩. ডিজিটাল সিগনেচার এবং এর তিনটি উদ্দেশ্য (Authentication, Integrity, Non-repudiation)
৪. ডিজিটাল সিগনেচারের কার্যপ্রণালী (হ্যাশ তৈরি, এনক্রিপশন ও যাচাইকরণ)
৫. ডিজিটাল সার্টিফিকেট ও Certificate Authority (CA)

এছাড়াও নিচের বিষয়গুলো সম্পর্কে বিশদভাবে জানতে ভিজিট করুন:

1. Key Management: https://www.geeksforgeeks.org/computer-networks/easy-key-management-in-cryptography/
2. Digital Signature: https://www.cisa.gov/news-events/news/understanding-digital-signatures
3. Digital Certificate & CA: https://www.digicert.com/blog/what-is-a-certificate-authority