রিজার্ভ চুরি : আবারও সেই একাত্তর!

মোস্তাফা জব্বার

গত ১৮ মার্চ বাংলাদেশ ব্যাংকের ঘটনা সম্পর্কে তদন্ত সংস্থা ফায়ারআই তাদের প্রাথমিক তদন্ত প্রতিবেদন প্রকাশ করেছে। দৈনিক প্রথম আলো ২০ মার্চ সেই আলোকে যে প্রতিবেদন প্রকাশ করে সেটি নিম্নরূপ :

'আগে থেকে বাংলাদেশ ব্যাংকের তথ্যপ্রযুক্তি বা আইটি ব্যবস্থার ত্রুটি জেনে এরপরই রিজার্ভের অর্থ চুরির সাইবার হামলাটি করা হয়েছে। বাংলাদেশ ব্যাংকের আইটি ব্যবস্থার নিরাপত্তায় যেসব ফায়ারওয়াল বা প্রতিরোধক ছিল, সেগুলোকে সহজে এরাতে বা বাইপাস করতে পারবে সাইবার আক্রমণের জন্য সেরকম 'বিশেষ প্রোগ্রাম' তৈরি করা হয়েছিল। যেটিকে 'সফিসটিকেটেড তথা অত্যাধুনিক ম্যালওয়্যার' হিসেবে আখ্যায়িত করা হচ্ছে। যুক্তরাষ্ট্রের নিউইয়র্কে ফেডারেল রিজার্ভ ব্যাংক থেকে বাংলাদেশ ব্যাংকের রিজার্ভের ১০ কোটি ১০ লাখ মার্কিন ডলার বা বাংলাদেশি মুদ্রায় প্রায় ৮০৮ কোটি টাকা চুরির ঘটনার অন্তর্বর্তীকালীন বা প্রাথমিক তদন্ত প্রতিবেদনে এসব তথ্য তুলে ধরা হয়েছে।

গত সপ্তাহের শেষ কার্যদিবস ১৮ মার্চে এ প্রতিবেদন দাখিল করা হয়েছে। তবে এ ঘটনার বিস্তারিত বা চূড়ান্ত প্রতিবেদন পেতে আরও দুই সপ্তাহ সময় লাগবে বলে জানানো হয়েছে। তদন্তে বলা হয়েছে, বাংলাদেশ ব্যাংকের দিক থেকে সুইফট ব্যবহারে নিযুক্ত কর্মকর্তারা সর্বশেষ পাসওয়ার্ড (গোপন নম্বর) পরিবর্তন করেছেন জানুয়ারির প্রথম সপ্তাহে। এরপর অর্থ চুরি যাওয়ার আগে আর পাসওয়ার্ড পরিবর্তনের তথ্য পাওয়া যায়নি। যুক্তরাষ্ট্রের সিলিকনভ্যালিভিত্তিক ফায়ারআই ও ভার্জিনিয়াভিত্তিক ওয়ার্ল্ড ইনফোমেট্রিকস সাইবার সিকিউরিটি যৌথভাবে এ রিজার্ভের অর্থ চুরির ঘটনার 'ফরেনসিক' (বৈজ্ঞানিক ও প্রযুক্তি ব্যবহার করে তথ্য-প্রমাণ উদঘাটন ও কার্যকারণ খুঁজে বের করা) তদন্ত করছে। মূলত বাংলাদেশ ব্যাংকের পক্ষ থেকে এ তদন্তের দায়িত্বভার দেয়া হয়েছে বিশ্বব্যাংকের সাবেক তথ্যপ্রযুক্তি কর্মকর্তা রাকেশ আস্থানার প্রতিষ্ঠান ওয়ার্ল্ড ইনফোমেট্রিকসকে। পরবর্তী সময়ে তার সাথে ফায়ারআইকে যুক্ত করা হয়।

এদিকে রাকেশ আস্থানাকে একটি প্রকল্পের আওতায় সাইবার বিশেষজ্ঞ হিসেবে নিয়োগ দিয়েছে বাংলাদেশ ব্যাংক। অন্তর্বর্তীকালীন তদন্ত প্রতিবেদনে বলা হয়েছে, বাংলাদেশ ব্যাংকের রিজার্ভের অর্থ চুরির জন্য যে সাইবার আক্রমণটি করা হয়েছে সেটি ছিল পূর্বপরিকল্পিত। এজন্য তথ্য চুরির সুবিধার্থে বিশেষভাবে তৈরি ম্যালওয়্যারটিতে কি (চাবি) লগারসসহ বাড়তি বিভিন্ন উপকরণ যুক্ত করা ছিল। ম্যালওয়্যার হচ্ছে এক ধরনের ক্ষতিকর বিশেষ সফটওয়্যার। ব্যক্তিগত কমপিউটারে প্রবেশাধিকার, গুরুত্বপূর্ণ তথ্য সংগ্রহ এবং কমপিউটারের স্বাভাবিক কার্যক্রম ব্যাহত করে হ্যাক করতে এটি ব্যবহার করা হয়। তদন্ত প্রতিবেদন অনুযায়ী, এখন পর্যন্ত কেন্দ্রীয় ব্যাংকের ৩২টি কমপিউটারে অত্যাধুনিক ম্যালওয়্যারের অস্তিত্ব খুঁজে পাওয়া গেছে, যেসব কমপিউটার বাংলাদেশ ব্যাংকের নিজস্ব বা অভ্যন্তরীণ নেটওয়ার্কের সাথে সংযুক্ত। এসব কমপিউটারের যেকোনো একটিকে ব্যবহার করে বাংলাদেশ ব্যাংকের নিজস্ব নেটওয়ার্কের মাধ্যমে আর্থিক লেনদেনের বার্তা বিনিময়কারী আন্তর্জাতিক নেটওয়ার্ক সুইফটে ঢুকে পড়েছিল তৃতীয় পক্ষটি। প্রাথমিক তদন্তের তথ্যানুযায়ী, তৃতীয় পক্ষটি সুইফটে ঢুকে গত ২৯ জানুয়ারি বেলা পৌনে ৩টার দিকে 'সুইফট লাইভ' কার্যক্রমের ভেতরে 'সিস্টেম মনিটরিং' সংক্ষেপে 'সিসমন' নামে অপর একটি প্রোগ্রাম বসিয়ে দেয়। এ 'সিসমন' প্রোগ্রামটি বসানোর আগেই সুইফট লাইভ ও সুইফট ইউএটি (ইউজার অ্যাসেফট্যানস টেস্ট) অ্যাডমিনিস্ট্রেটরের (প্রশাসক) নিয়ন্ত্রণ নিয়ে নেয়।

বিশেষজ্ঞরা বলছেন, কমপিউটারের কোনো একটি সিস্টেম ও নেটওয়ার্কে যিনি অ্যাডমিন থাকেন, পুরো সিস্টেমটির নিয়ন্ত্রণ থাকে তার হাতে। ওই অ্যাডমিন সিস্টেমটিতে যেকোনো কিছু সংযোজন, বিয়োজন, পরিবর্তনসহ যাবতীয় কার্যক্রম চালাতে পারেন। কিন্তু অ্যাডমিন ছাড়া ওই সিস্টেম বা নেটওয়ার্ক ব্যবহারকারীরা নির্ধারিত কিছু কাজ ছাড়া বাড়তি কিছু করতে পারেন না। ব্যবহারকারীরা কী কী কাজ সিস্টেমে করতে পারবেন তা অ্যাডমিনই নির্ধারণ করে দেন। ফায়ারআই ও ওয়ার্ল্ড ইনফোমেট্রিকসের যে প্রাথমিক তদন্ত প্রতিবেদন, সেটির কারিগরি দিকগুলো নিয়ে প্রথম আলোর পক্ষ থেকে বাংলাদেশ প্রকৌশল বিশ্ববিদ্যালয়ের (বুয়েট) সহযোগী অধ্যাপক এবং কমপিউটার নেটওয়ার্ক ও সিকিউরিটি সিস্টেম বিশেষজ্ঞ ইউসুফ সারোয়ারসহ বুয়েটের একাধিক বিশেষজ্ঞের মতামত নেয়া হয়েছে।

প্রাথমিক তদন্ত প্রতিবেদনের কারিগরি বিভিন্ন বিষয় বিশ্লেষণ করে ইউসুফ সারোয়ার প্রথম আলোকে বলেন, তদন্তের ভাষ্য অনুযায়ী অর্থ চুরিতে ব্যবহৃত 'ম্যালওয়্যারটি' বাংলাদেশ ব্যাংকের রিজার্ভের সিস্টেম হ্যাক করার জন্য বিশেষভাবে তৈরি। এ কারণে সহজে ফায়ারওয়াল বা প্রতিরোধকগুলো ভেদ করতে পেরেছে। তদন্ত প্রতিবেদনে বলা হয়েছে, বাংলাদেশ ব্যাংকের সুইফট সিস্টেমে যে সিসমন প্রোগ্রাম বসানো হয়েছিল, সেটি ২৯ জানুয়ারি সারাদিনই সচল থাকার তথ্য-উপাত্ত মিলেছে। তবে হ্যাকারেরা বাংলাদেশ ব্যাংকের নিজস্ব নেটওয়ার্ক ও সুইফট সিস্টেম থেকে অনেকগুলো তথ্য-উপাত্ত মুছে ফেলেছে। যাতে তাদের উপস্থিতি-সংক্রান্ত তথ্যগুলো সংরক্ষিত না থাকে। তবে তদন্তকারী সংস্থার পক্ষ থেকে বলা হয়েছে, বিশেষ প্রোগ্রাম ব্যবহার করে মুছে ফেলা তথ্য পুনরুদ্ধারের চেষ্টা চলছে। সিসমনের বিষয়ে জানতে চাইলে ইউসুফ সারোয়ার প্রথম আলোকে বলেন, 'সিসমন' এমন একটি প্রোগ্রাম, যার মাধ্যমে অপর একটি সিস্টেমের যাবতীয় কার্যক্রমের তথ্য সংগ্রহ ও সংরক্ষণ করা হয়। সিসমনে যেভাবে তথ্য সংরক্ষণ করা হয়, সেগুলো পরবর্তী সময়ে ম্যালওয়্যারের মাধ্যমে অত্যন্ত গোপনীয়তার সাথে হ্যাকারেরা নিজেদের মধ্যে বিনিময় বা ভাগাভাগি করতে পারে। এদিকে ফরেনসিক প্রতিবেদনে বাংলাদেশ ব্যাংকের সিস্টেমে তৃতীয় পক্ষের উপস্থিতির ক্রমানুযায়ী কিছু বিবরণ দেয়া হয়েছে। তাতে সন্দেহজনক তৃতীয় পক্ষের প্রথম উপস্থিতি পাওয়া গেছে ২৪ জানুয়ারি। ওইদিন দুই দফায় এ উপস্থিতির তথ্য-উপাত্ত পাওয়া গেছে। প্রথম দফায় মাত্র ৫৫ সেকেন্ড এবং দ্বিতীয় দফায় ১ মিনিট ৩৭ সেকেন্ড ধরে উপস্থিতি ছিল তৃতীয় পক্ষটির। এরপর ২৯ জানুয়ারি দীর্ঘ সময়ের উপস্থিতি ছিল ওই পক্ষটির। ওইদিন সুইফট থেকে তথ্য সংগ্রহের জন্য বাড়তি একটি প্রোগ্রাম বসানো হয়েছিল। ২৯ জানুয়ারির পর আবারও তৃতীয় পক্ষটির অস্তিত্ব পাওয়া গেছে ৩১ জানুয়ারি। ওইদিন বেশ কয়েক দফায় উপস্থিতির তথ্য-প্রমাণ রয়েছে। ফরেনসিক তথ্য-প্রমাণের ভিত্তিতে তদন্ত প্রতিবেদনে বলা হয়েছে, প্রকৃত ব্যবহারকারীর পরিচিতির তথ্য চুরি করে তা কাজে লাগে কি না, সেটি যাচাই করে দেখা হয় ৩১ জানুয়ারি। এরপর ▸