# বাংলাদেশ ব্যাংক কেলেঙ্কারি: লুটপাট, মিথ্যাকথন ও হাস্যরস

তারিফ রিয়াদ রহমান

*সবচাইতে সুরক্ষিত থাকার কথা যে প্রতিষ্ঠানের সেখানকার বৈদেশিক তহবিলে বাটপারদের প্রবেশ করবার মতো অবিশ্বাস্য ঘটনাও ঘটেছে। আর এর খবর দেশের কেউ প্রকাশ করেনি, কর্তৃপক্ষও না। বিদেশি পত্রিকায় প্রকাশের পর এদেশের মানুষ জেনেছেন। তদন্ত কমিটিও হয়েছে ঘটনার এক মাস পর। আসলে ঘটনা কী? এখানে বাংলাদেশ ব্যাংক ও সরকারের দায়িত্ব কী? রহস্যঘেরা জটিল বিষয়কে অনুসন্ধান করা হয়েছে এই প্রবন্ধে।*

এক অনাড়ম্বর বিদায়ের মধ্য দিয়ে বাংলাদেশ ব্যাংকের সাবেক গভর্নর আতিউর রহমানের মেয়াদ শেষ হলো। সরকারপক্ষ থেকে তাঁর বিদায়কে 'সাহসী' আখ্যা দেওয়ার চেষ্টা করা হয়েছিল; তবে নজিরবিহীন কলঙ্কের কালিমা রাজনৈতিকভাবে এমনই অমোচনীয় ছিল যে ক্ষমতার সর্বোচ্চ স্তরে থাকা তাঁর পৃষ্ঠপোষকদের পক্ষেও তাঁকে বিদায় দেওয়া ছাড়া উপায় ছিল না। অন্যদিকে কলঙ্ক থেকে বাঁচতে অর্থমন্ত্রীর 'রাবিশ'গিরি করতে ভুল হয়নি। সাদা চোখে আলাদা লাগলেও অর্থমন্ত্রী ও বিদায়ী গভর্নর– উভয়ের মধ্যে অনেক মিল রয়েছে। দুজনই বাংলাদেশের উন্নয়ন প্রশ্নে তথাকথিত উন্নতির কিছু পরিসংখ্যান প্রাণপণে আঁকড়ে ধরে রাখেন এবং বৈদেশিক মুদ্রার রিজার্ভের সাধ্যমতো গুণকীর্তন করেন; অবশ্য গভর্নরের সততা নিয়ে এখন তাঁর গুণগ্রাহী ও পৃষ্ঠপোষকরাই সন্দেহ করছেন। এই সাথে এ দুই ব্যক্তির নেতৃত্বে বাংলাদেশের ইতিহাসের সবচেয়ে বড় ব্যাংক কেলেঙ্কারির ঘটনা ঘটেছে, যার এমনকি কোনো লোকদেখানো বিচারও হয়নি। এখন আবার দেখা যাচ্ছে উন্নয়নের 'দিশারি' আখ্যা দিয়ে যে ডলার রিজার্ভের গর্ব করা হয়, সেটিও নিরাপদ নয়। এতসব কেলেঙ্কারির পর বাংলাদেশের চলতি হিসাব থেকে ১০০ মিলিয়ন ডলার লুট হয়ে যাওয়ার ঘটনা যেন 'রাজমুকুটে নতুন পালক'। তবে ঘটনা-পরবর্তী প্রতিক্রিয়া এবং ধীরে ধীরে বিস্তারিত যে বিবরণ উন্মোচিত হচ্ছে, তাতে মনে হয় আরো অনেক প্রশ্ন রয়েই গেছে।

এই সাথে এ দুই ব্যক্তির নেতৃত্বে বাংলাদেশের ইতিহাসের সবচেয়ে বড় ব্যাংক কেলেঙ্কারির ঘটনা ঘটেছে, যার এমনকি কোনো লোকদেখানো বিচারও হয়নি। এখন আবার দেখা যাচ্ছে উন্নয়নের 'দিশারি' আখ্যা দিয়ে যে ডলার রিজার্ভের গর্ব করা হয়, সেটিও নিরাপদ নয়।

এই মহালোপাটের ঘটনা ঘটার এক মাস পর খবর ফাঁস হয়। এবং আশ্চর্য নয় যে ফিলিপাইনের পত্রপত্রিকায় খবরটি ছাপানোর পরই বাংলাদেশের মিডিয়ায় এ নিয়ে রিপোর্ট হয়–পুরো ঘটনা নিয়ে ফিলিপাইনের দৈনিক এনকোয়ারার প্রথম প্রতিবেদন করেছিল। সাধারণ মানুষ এসব নিয়ে যখন প্রতিবাদ ও প্রতিক্রিয়া দেখানো শুরু করল, কেবল তখনই সরকারকে কিছু আপাতকঠোর হতে দেখা গেল; অবশ্যই বিব্রত হওয়ার কারণে। অর্থ লুটের পরিণাম বিশ্লেষণের স্বার্থে এই ঘটনার পূর্বাপর একবার স্মরণ করা ও বোঝা দরকার।

ফিলিপাইনের দৈনিক এনকোয়ারার সর্বপ্রথম ২৯ ফেব্রুয়ারি ওই দেশের ভেতরে ১০০ মিলিয়ন ডলার পাচার হওয়ার একটি প্রতিবেদন প্রকাশ করে। ইচ্ছাকৃতভাবে নয়, এনকোয়ারার প্রতিবেদনটি প্রকাশ করে স্থানীয় মানি লন্ডারিং প্রতিরোধ কাউন্সিলের (এএমএলসি) অনুরোধে এবং তাদের চলমান তদন্ত এবং এ সম্পর্কিত দ্বিধা নিরসনের স্বার্থে। বাংলাদেশের ঢাকা ট্রিবিউন 'ব্যাংক লুটের ব্যবচ্ছেদ' শিরোনামে লুটপাটের ঘটনার বিস্তারিতসহ একটি চমৎকার প্রতিবেদন প্রকাশ করে। উভয় প্রতিবেদন অনুসারে, মার্কিন ডলারের অ্যাকাউন্ট খোলা হয়েছিল গত বছরের ১৫ মে। এ বছরের ৪ ফেব্রুয়ারি পর্যন্ত অ্যাকাউন্টগুলো নিষ্ক্রিয় ছিল। ফিলিপাইনের রিজাল কমার্শিয়াল ব্যাংকিং করপোরেশন (আরসিবিসি) নামের একটি স্থানীয় ব্যাংকে ভুয়া ঠিকানা ও কাগজপত্র ব্যবহার করে স্থানীয় ফিলিপিনো নাগরিকদের নামে রেজিস্টার করে অ্যাকাউন্টগুলো চালু করা হয়। ফলে নিউ এজের রিপোর্ট অনুযায়ী, এএমএলসি ও ফিলিপিনো সিনেট তদন্ত শুরু করলে দেখা গেল, সংশ্লিষ্ট চার ব্যক্তিকে তলব করার কোনো উপায় নেই।

লুটপাটের কথায় ফেরা যাক–অর্থ স্থানান্তরের পুরো বিষয়টি নিঃসন্দেহে দুঃসাহসী এবং মহারথীদের বেফাঁস বানান ভুল ধরা পড়ার আগ পর্যন্ত নিখুঁত ছিল। এমন নিখুঁত টাইমিং আর হয় না। ফেব্রুয়ারির ৪ তারিখ বৃহস্পতিবার বাংলাদেশে সাপ্তাহিক ছুটির (শুক্র ও শনিবার) আগের দিন। ওদিকে চীনা নতুন বছর উদ্‌যাপন উপলক্ষে পরবর্তী সোমবার বন্ধ থাকায় ফিলিপাইনেও লম্বা সাপ্তাহিক ছুটি শুরু হচ্ছিল। দারুণ চৌর্যবৃত্তিক দক্ষতার সাথে পুরো অপারেশনটি চালানো হয়েছিল। ডয়চে ভেলে সংবাদ সংস্থার প্রতিবেদন অনুযায়ী, অপরাধীরা বিবিধ পরিমাণ অর্থ বিভিন্ন দেশের বিভিন্ন অ্যাকাউন্টে পাঠানোর উদ্দেশ্যে মার্কিন ফেডারেল রিজার্ভ[১] বরাবর সর্বমোট এক বিলিয়ন ডলারের ৩০টি উপর্যুপরি ট্রান্সফার রিকোয়েস্ট পাঠিয়েছিল।

প্রায় ৩০টি ট্রান্সফার রিকোয়েস্টের মধ্যে চারটিতে কাজ হয়, যার পরিমাণ প্রায় ৮১ মিলিয়ন ডলার। আরসিবিসির চারটি[২] সন্দেহজনক ডলার অ্যাকাউন্টে সেই অর্থ জমা হয়। পঞ্চম ট্রান্সফার রিকোয়েস্টটি শ্রীলঙ্কায় 'শ্রীলিখা ফাউন্ডেশন' নামক ভুয়া একটি এনজিওর রেজিস্ট্রিকৃত অ্যাকাউন্টে যাওয়ার কথা ছিল। সে সময় সতর্ক হয়ে পড়ায় লুটপাটের পথে হঠাৎ আপদ দেখা দিল। পঞ্চম লেনদেনের অনুরোধে লুটেরারা ফাউন্ডেশন বানান ভুলক্রমে 'ফান্ডেশন' (fandation) লিখে পাঠালে ডয়েচ ব্যাংক (তৃতীয় যে ব্যাংকে অর্থ পাচার হচ্ছিল) লেনদেন বন্ধ রাখে। তবে একজন প্রত্যক্ষদর্শীর বরাতে আমরা জানতে পারি, প্রাপক শ্রীলঙ্কার ব্যাংকের যাচাইকরণ অনুরোধ প্রাপ্তি সাপেক্ষে লেনদেন শুধুমাত্র স্থগিত রাখা হয়। এদিকে ক্রমাগত লেনদেনের অনুরোধ আসছিল। গার্ডিয়ানের প্রতিবেদন অনুযায়ী, অস্বাভাবিক উচ্চ সংখ্যার অনুরোধ এবং সব ট্রান্সফার ব্যক্তিগত অ্যাকাউন্টে হওয়ায় মার্কিন ফেডারেল রিজার্ভের সন্দেহ হয়।

ডয়েচে ব্যাংক ও ফেডারেল রিজার্ভ থেকে সতর্কবার্তা বাংলাদেশ ব্যাংকে পাঠাতে পাঠাতে অনেক দেরি হয়ে যায়। ৮১ মিলিয়ন ডলার ইতিমধ্যে ফিলিপাইনে পাচার হয়ে যায়। এর মধ্যে কে কত অর্থ পেয়েছে তা নিচের টেবিলে দেখানো হলো :

| অ্যাকাউন্টধারীর নাম | পরিমাণ |
|---|---|
| জেসি ক্রিস্টোফার লাগরোসাস | ৩০ মিলিয়ন ডলার |
| আলফ্রেড স্যান্টোস ফারগারা | ১৯.৯৯ মিলিয়ন ডলার |
| এনরিকো থিওডর ভাস্কুয়েজ | ২৫ মিলিয়ন ডলার |
| মাইকেল ফ্রান্সিসকো ক্রুজ | ৬ মিলিয়ন ডলার |

টেবিল-১ : বাংলাদেশ ব্যাংকের তহবিল লুট। সূত্র : ঢাকা ট্রিবিউন

এই বিপুল অর্থ ৪ ফেব্রুয়ারি আরসিবিসিতে চলে গেলে লাগরোগাস সেখান থেকে ২২.৭৩ মিলিয়ন ডলার উত্তোলন করেন এবং পুরোটা চীনা ব্যবসায়ী উইলিয়াম হোর মার্কিন ডলার অ্যাকাউন্টে জমা করেন, যে অ্যাকাউন্টটি মাত্র সেদিনই খোলা হয়েছিল। হো একজন জাংকেট অপারেটর। একজন জাংকেট[৩] অপারেটরের অ্যাকাউন্টে অর্থ স্থানান্তরিত হওয়া কোনো কাকতলীয় ঘটনা নয়, বরং অত্যন্ত পরিকল্পিত। এএমএলসির নিজস্ব আইনি কাঠামোর সীমার পেছনে রয়েছে ফিলিপাইনের ক্যাসিনো ও জুয়াড়ি সংগঠনগুলো।

২৩ মিলিয়ন ডলার লুট হয়ে গেলেও ক্ষণিকের জন্য মনে হয়েছিল, বাকি ৫৮ মিলিয়ন ডলার উদ্ধার করা সম্ভব। ডয়েচে ব্যাংক ও মার্কিন ফেডারেল রিজার্ভ থেকে সতর্কবার্তা পাওয়ার সাথে সাথে বাংলাদেশ ব্যাংক লেনদেন বন্ধ এবং অধিকতর তদন্তের স্বার্থে অ্যাকাউন্টগুলো ফ্রিজ করার অনুরোধ জানিয়ে আরসিবিসিকে সুইফট[৪] বার্তা পাঠায়। ঘটনাক্রমে সুইফট বার্তাগুলো ৮ তারিখে পাঠানো হয়–ফিলিপাইনে সেদিন ছুটির দিন ছিল। পরের দিন ৯ ফেব্রুয়ারি নিশ্চিত হওয়া যায় যে আরসিবিসি বাংলাদেশ ব্যাংকের সুইফট বার্তাগুলো পেয়েছে। ঠিক তখন থেকেই ঘটনাধারা অস্পষ্ট হতে শুরু করে। পরে আমরা জানতে পারি যে বাকি ৫৮ মিলিয়ন ডলার ফিলিপিনস রেমিট্যান্স করপোরেশন (PhilRem Corp.) কর্তৃক রেমিট্যান্স আকারে স্থানীয় মুদ্রা পেসোয় রূপান্তরিত হয়েছে। জনৈক ওয়াইকান জু নামের একজন চীনা নাগরিক এবং স্বভাবতই জাংকেট অপারেটরের অ্যাকাউন্টে অর্থ জমা করা হয়। আরসিবিসির আদেশক্রমে অর্থ পরিশোধিত হয়। তবে বাংলাদেশ ব্যাংকের সুইফট বার্তা পাওয়ার আগে না পরে আদেশ দেওয়া হয়েছিল, সেটির সুরাহা হয়নি।

> দু-একটা ব্যতিক্রম ছাড়া দেশীয় মিডিয়ার খবরে যতটা চটকদারি বা নাটকীয়তা ছিল, ততটা নিয়মনিষ্ঠা মোটেই ছিল না।

বাংলাদেশ ব্যাংকের গভর্নর আতিউর রহমানের হাতে ফিলিপাইনের ব্যাংকিং কর্তৃপক্ষ ও সংশ্লিষ্ট গভর্নরের সাথে যোগাযোগ করা ছাড়া উপায় ছিল না। কেবলমাত্র তখনই এএমএলসি নামক প্রতিষ্ঠানটিকে সংশ্লিষ্ট অ্যাকাউন্টগুলো আদালতের নিষেধাজ্ঞা এনে স্থগিত করতে একেবারে উঠেপড়ে লাগতে দেখা গেল। তবে অর্থপাচারের আদর্শ নকশা অনুযায়ী আমরা জানি, এ ধরনের অর্থ সব সময় স্থানীয় কর্তৃপক্ষের আইনি সীমার বাইরে চালান করে দেওয়া হয় এবং বাংলাদেশ ব্যাংক কর্মকর্তাদের ধারণা, সমুদয় অর্থ ইতিমধ্যে হংকংয়ে পাচার হয়ে গেছে। এএমএলসির হস্তক্ষেপের পর পুরো বিষয়টি তদন্ত করতে একটি সিনেট কমিটি গঠন করা হয়। সিনেট কমিটি সংশ্লিষ্ট ব্যক্তিদের তলব করলে দেখা গেল, পুরো বিষয়টি একটি চক্রের মধ্যে ঘুরপাক খাচ্ছে। প্রত্যেক সাক্ষী অন্য কারো ওপর দোষ চাপানোর চেষ্টা করছে। আরসিবিসি কর্মকর্তাদের ডেকে সন্দেহজনক অ্যাকাউন্ট বিষয়ে জানতে চাওয়া হলে বাস্তবে লুটপাটের ঘটনাগুলো কৌশলে আড়াল করলে তাঁরা ব্যাংক গোপনীয়তা আইনের দোহাই দিচ্ছেন।

এএমএলসি জাংকেট অপারেটর কিম অংসহ আরো কিছু ব্যাংক অ্যাকাউন্ট ফ্রিজ বা স্থগিত করে এবং তাঁকে সিনেট কমিটির সামনে ডাকা হয়। ৩১ মার্চ পর্যন্ত তিনি পাচারকৃত অর্থ থেকে ৪.৬ মিলিয়ন ডলার এএমএলসির কাছে সমর্পণ করেন। ধারণা করা হয়, তাঁর কোম্পানির কাছে আরো অতিরিক্ত ১০ মিলিয়ন ডলার আছে। অন্যদিকে PhilRem Corp. নামক প্রতিষ্ঠানটি পাচারকৃত অর্থের রেমিট্যান্সজাত মুনাফা বাংলাদেশকে ফেরত দিতে সম্মত হয়েছে, যার পরিমাণ প্রায় আড়াই লাখ ডলার।

এসব ঘটনাবলি থেকে ফিলিপাইন রাষ্ট্রের ভূমিকা অনেকের কাছেই প্রশংসনীয় মনে হতে পারে। প্রজ্ঞা ও দ্রুততার সাথে এএমএলসিকে এই ঘটনায় যুক্ত করা এবং সিনেট কমিটি গঠন করা একটি ভালো উদাহরণ। তবে আরো কিছু কারণ বিবেচনায় নিলে ফিলিপাইন রাষ্ট্রযন্ত্রের এমন আচরণ অস্বাভাবিক মনে হয় না। ২০১৬ সাল ফিলিপাইনের নির্বাচনী বছর এবং বর্তমান রাষ্ট্রপতি তৃতীয় বেনিগনো একুইনো তাঁর মেয়াদ শেষ হলে পদত্যাগ করবেন। একই সাথে বিশ্বব্যাংকের হিসাব অনুযায়ী ফিলিপাইন হলো ৩০ বিলিয়ন ডলারের তৃতীয় বৃহত্তম রেমিট্যান্সপ্রাপ্ত দেশ এবং সে দেশের বহু প্রবাসী শ্রমিক ফিলিপাইনের রেমিট্যান্স কোম্পানিগুলোর মাধ্যমে তুলনামূলক কম কমিশনের বিনিময়ে দেশে অর্থ পাঠায়। এইসব কোম্পানির অনেকগুলোই গত কয়েক বছরে প্রবাসী শ্রমিক নেওয়া দেশগুলো কর্তৃক কালো তালিকাভুক্ত হয়েছে। ফলে গড়পড়তা একজন শ্রমিককে অধিক অর্থের বিনিময়ে দেশে অর্থ পাঠাতে হচ্ছে। একে বিশ্বের অন্যতম গরিব ও দুর্নীতিগ্রস্ত দেশ, মানবাধিকার পরিস্থিতিও খুব একটা ভালো নয়, তার ওপর প্রবাসীদের প্রত্যাশার চেয়ে কম অর্থ পাঠানো যেন হয়েছে মড়ার ওপর খাঁড়ার ঘা। ফলে একুইনোর লিবারেল পার্টির ভয়ানক গণরোষের মুখে পড়ার ঝুঁকি আছে এবং স্বভাবতই তিনি তা চাইবেন না। ফলে বাংলাদেশ ব্যাংক ইস্যুতে আমরা পুরো রাষ্ট্রযন্ত্রকে ঝাঁপিয়ে পড়তে দেখি। এখানে পরার্থপরতার কিছু নেই; পুরোটাই স্বার্থ। বাংলাদেশের কপাল ভালো বলা যায় যে দেশটি ফিলিপাইন ছিল।

এ পর্যন্ত টাকা পাচার ও স্থানান্তরের ডায়নামিকস ও মেকানিকসটা বোঝা যায়, কিন্তু এর সাথে বাংলাদেশের সম্পর্ক কী, মিডিয়ার প্রতিবেদন বা অভিযোগ থেকে তা বোঝা যায় না। শুরুতে কে ও কিভাবে ফেডারেল রিজার্ভে বাংলাদেশের চলতি অ্যাকাউন্ট থেকে অর্থ স্থানান্তরের ট্রান্সফার রিকোয়েস্ট পাঠিয়েছিল? এই 'কে'টা নিয়ে নিশ্চিত হওয়া এই মুহূর্তে বেশ কঠিন। তবে আমরা–যেহেতু সমস্ত ঘটনা এই মুহূর্তে আমাদের জানা নেই–একটি অত্যন্ত সম্ভাব্য উপায়ে 'কিভাবে' প্রশ্নের উত্তর খুঁজে দেখতে পারি।

বাংলাদেশ ব্যাংকের তহবিল লুটপাটের খবর জানাজানি হলে প্রথমে এটিকে চীনা হ্যাকারদের কাজ বলে খবর জানা গেল। ব্যাংকের একজন নির্বাহীর বরাত দিয়ে ফিলিপাইনের এনকোয়ারার পত্রিকায় প্রথম রিপোর্ট এলো। এই রিপোর্টের তথ্য থেকে বাংলাদেশসহ বিশ্বের অন্যান্য মিডিয়ায় খবর প্রকাশিত হলো। এটা কি হ্যাকিং ছিল না অন্য কিছু; এবং হ্যাকিং যদি হয়, অভিযুক্তরা চীনা না অন্য

কেউ–এসব বিষয় কখনোই প্রতিপন্ন করা হয়নি। অধিকাংশ পত্রপত্রিকার রিপোর্ট যেন মার্কিন সেই টিভি সিরিয়াল মিস্টার রোবটের মতো, যেখানে দেখানো হয় নায়ক ইলিয়ট এন্ডারসন খলনায়ক এভিল কর্প. হ্যাক করে পুরো কাঠামো ধ্বংস করছে। দু-একটা ব্যতিক্রম ছাড়া দেশীয় মিডিয়ার খবরে যতটা চটকদারি বা নাটকীয়তা ছিল, ততটা নিয়মনিষ্ঠা মোটেই ছিল না।

আসল কথায় ঢোকার আগে নিজেদের একটি সহজ প্রশ্ন জিজ্ঞেস করা যাক। মানুষ হ্যাকার কিভাবে হয়? গুগলের সংজ্ঞা অনুযায়ী, হ্যাকার হলেন তিনি, যিনি 'কম্পিউটারের মাধ্যমে অপরজনের তথ্যে অনধিকার প্রবেশ করেন'। পরের প্রশ্নটি হলো, কী চুরি হয়েছে এবং কোথা থেকে চুরি করার অভিযোগ উঠেছে? হ্যাঁ, এবার আমরা বিষয়ের মূল জায়গায় আসতে পারব।

একটা বিষয় পরিষ্কার যে বাংলাদেশ ব্যাংক থেকে সহজাতভাবে কোনো কিছু চুরি হয়নি। চুরি হয়েছে ইলেকট্রনিক মানি–মার্কিন ফেডারেল রিজার্ভে বাংলাদেশ ব্যাংকের চলতি হিসাব থেকে। চুরিটা কিভাবে হলো? হয়েছে বাংলাদেশ ব্যাংক প্রতিনিধির রূপধারী কোনো ব্যক্তির মার্কিন ফেডারেল রিজার্ভে ট্রান্সফার রিকোয়েস্ট পাঠানোর মাধ্যমে। ট্রান্সফার রিকোয়েস্ট কিভাবে পাঠানো হলো? অবশ্যই কোনো ফোনকল বা লিখিত মেমোর মাধ্যমে নয়। বিশ্বজুড়ে সমস্ত রকমের আন্তব্যাংক লেনদেন এবং এ সংক্রান্ত বার্তা আদান-প্রদানের কাজে ব্রাসেলসভিত্তিক সুইফট (SWIFT) প্রটোকল ব্যবহৃত হয়। দাবি করা হয় যে অর্থনৈতিক বার্তা নিরাপদে আদান-প্রদানের প্রশ্নে এটি বিশ্বের সেরা মাধ্যম।

ফলে এটা পরিষ্কার যে সুইফটের মাধ্যমে অর্থ স্থানান্তর করতে হলে থ্রিএসকি ডিভাইস, পাসওয়ার্ড ও পাবলিক-প্রাইভেট কি ছাড়া অসম্ভব। 'থ্রিএসকি ডিভাইস অথেনটিকেশনের পুরনো পদ্ধতি' বলার মাধ্যমে বাংলাদেশ ব্যাংক আসলে কী বলতে চাইছে, সেটাও পরিষ্কার নয়, কারণ সুইফট এই সেবা দিচ্ছে মাত্র ২০১২ সাল থেকে।

### সুইফটের মাধ্যমে কিভাবে আন্তব্যাংক লেনদেন হয়?

সুইফটের ওয়েবসাইট থেকে দেখা যাচ্ছে, ব্যবহারকারীদের সঠিকতা প্রমাণ ও যাচাই করতে তারা একটি পাবলিক কি ইনফ্রাস্ট্রাকচার মেকানিজম ব্যবহার করে থাকে। সুইফটভিত্তিক অর্থ লেনদেনের ক্ষেত্রে প্রত্যেক ব্যবহারকারী একটি 'ডিজিটাল সিগনেচার' বা কিছু ফাইল পাবেন। এসব ফাইলই হলো আসলে পাবলিক ও প্রাইভেট কি। এগুলো আসলে কী জিনিস? এসবের কাজ কী? পাবলিক ও প্রাইভেট কি হলো কিছু সংখ্যার গুচ্ছ, যেখানে প্রতিটি সংখ্যা আবার বিপুলসংখ্যক ডিজিটের সমন্বয়ে গঠিত হয়। পাবলিক ও প্রাইভেট কিগুলো গাণিতিকভাবে পরস্পর সম্পর্কিত।

ধরা যাক, বাংলাদেশ ব্যাংক মার্কিন ফেডারেল রিজার্ভে একটি অর্থনৈতিক বার্তা পাঠাতে চায়। সে ক্ষেত্রে বার্তাটি প্রথমে সাধারণ ইংরেজিতে লিখতে হবে। এই বার্তাটি গাণিতিক পরিবর্তনের মাধ্যমে এমন একটি রূপ নেয়, যা মূল বার্তাটিকে আড়াল করে। পাবলিক কি ব্যবহার করে গাণিতিক পরিবর্তনটি করতে হয়।

এখন বাংলাদেশ ব্যাংক যদি মার্কিন ফেডারেল রিজার্ভে অর্থনৈতিক বার্তা পাঠাতে চায়, তাহলে অবশ্যই তাকে মার্কিন ফেডারেল রিজার্ভের পাবলিক কি ব্যবহার করে গাণিতিক পরিবর্তনটি করতে হবে। সুইফটের সদস্য প্রতিটি প্রতিষ্ঠানের নিজস্ব ডিজিটাল সিগনেচার আছে, যেটি সরবরাহ করে সুইফট কর্তৃক অনুমোদিত একটি সার্টিফিকেট কর্তৃপক্ষ। একটি প্রতিষ্ঠানের পাবলিক কি বাকি সদস্য প্রতিষ্ঠানগুলোর জানা থাকে, কিন্তু প্রত্যেকের প্রাইভেট কি সব সময় গোপন থাকে। বাংলাদেশ ব্যাংকের এনক্রিপটেড বার্তা পাওয়ার পর ফেডারেল রিজার্ভ কেবলমাত্র নিজস্ব প্রাইভেট কি ব্যবহার করে ডিক্রিপ্ট করে মূল বার্তাটি পড়তে পারবে। একইভাবে মার্কিন ফেডারেল রিজার্ভের বাংলাদেশ ব্যাংকে কোনো ফিরতি বার্তা পাঠানোর দরকার হলে অবশ্যই বাংলাদেশ ব্যাংকের পাবলিক কি ব্যবহার করে বার্তা এনক্রিপটেড করে পাঠাতে হবে এবং বাংলাদেশ ব্যাংক তার নিজস্ব প্রাইভেট কি ব্যবহার করে বার্তাটি ডিক্রিপ্ট করে পড়তে পারবে।

হ্যাকার এনক্রিপটেড বার্তা যদি হ্যাক করেও থাকে, তবু গ্রহীতার প্রাইভেট কি হাত করতে না পারলে বার্তাটি ডিক্রিপ্ট করতে পারবে না। অন্য যে উপায়ে হ্যাকাররা প্রাইভেট কির জন্য চেষ্টা করতে পারে তা হলো পাবলিক কির ওপর ক্রমাগত গাণিতিক অপারেশন চালিয়ে যাওয়া; অর্থাৎ সংখ্যার ক্রমাগত বিন্যাস-সমাবেশ চালাতে থাকা, যতক্ষণ পর্যন্ত সঠিক সমাবেশ না মিলছে। তবে এই সমাধান তাত্ত্বিকভাবে সম্ভব হলেও বাস্তবে অসম্ভব। যেমন–২০০৯ সালে এই পদ্ধতি পরীক্ষার জন্য বিশেষজ্ঞরা ১০০টি কম্পিউটার থেকে চেষ্টা শুরু করেন এবং সঠিক সমাবেশ দিয়ে ২৩২ ডিজিটের আদর্শ কি ভাঙতে তাঁদের দুই বছর সময় লাগে। এখন এ ধরনের আদর্শ কি হয় ৬১৭ ডিজিটের, কাজেই বোঝা যাচ্ছে এত কম সময়ে বাংলাদেশ ব্যাংকের প্রাইভেট কি ভাঙা অসম্ভর ব্যাপার।

সুইফট অথেনটিকেশন বা প্রমাণের জন্য ডিজিটাল সার্টিফিকেট একমাত্র উপায় নয়। অর্থ স্থানান্তরের বার্তা পাঠাতে বা পেতে হলে ব্যবহারকারীকে অবশ্যই প্রথমে তাঁর ইউজার নেম ও পাসওয়ার্ড দিতে হবে। এক্ষেত্রে ইউজার নেম ও পাসওয়ার্ড সুইফট প্রদত্ত একটি সফটওয়্যারে প্রবেশ করাতে হয়, যেখানে আবার ইউজার নেম টাইপ করা যায় না; বরং সুইফট প্রদত্ত একটি থ্রিএসকি ডিভাইস কম্পিউটারে প্রবেশ করাতে হয়। থ্রিএসকি হলো এক ধরনের ইউএসবি ডিভাইস, যেটি লগ ইন করার সময় অনন্য টোকেন নম্বর বা ইউজার নেম তৈরি করে। অর্থাৎ অর্থ স্থানান্তর প্রক্রিয়ায় সুইফট সিস্টেম বাড়তি স্তরের নিরাপত্তা দেয়, কারণ ডিভাইস কম্পিউটারে ঢোকাতে হলে ব্যক্তিকে শারীরিকভাবে উপস্থিত থাকতে হবে। একমাত্র ইউজার নেম ও পাসওয়ার্ড সঠিক প্রমাণিত হলেই পাবলিক-প্রাইভেট কি ব্যবহার করে বার্তা বিনিময় করা সম্ভব। ফলে এটা পরিষ্কার যে সুইফটের মাধ্যমে অর্থ স্থানান্তর করতে হলে থ্রিএসকি ডিভাইস, পাসওয়ার্ড ও পাবলিক-প্রাইভেট কি ছাড়া অসম্ভব। 'থ্রিএসকি ডিভাইস অথেনটিকেশনের পুরনো পদ্ধতি' বলার মাধ্যমে বাংলাদেশ ব্যাংক আসলে কী বলতে চাইছে, সেটাও পরিষ্কার নয়, কারণ সুইফট এই সেবা দিচ্ছে মাত্র ২০১২ সাল থেকে।

### বাংলাদেশ ব্যাংক লুটপাট কি আসলেই হ্যাকিং?

শেষমেশ এই চুরির খবর বাংলাদেশে চাউর হলে অর্থমন্ত্রী ক্ষিপ্ত হয়ে যাকে পান তাকেই দোষারোপ করা শুরু করলেন–কিছু বাদ রাখলেন না। তিনি এমনকি নিউ ইয়র্কে মার্কিন ফেডারেল রিজার্ভের নামে মামলা করারও হুমকি দিলেন। সুইফট ও মার্কিন ফেডারেল রিজার্ভ নিউ ইয়র্কের প্রধানরাও তৎক্ষণাৎ মিথ্যা খণ্ডন করে বক্তব্য দিলেন।

দুই প্রধান কর্মকর্তার মাধ্যমে আমরা নিশ্চিত হলাম যে কোনো প্রতিষ্ঠানেই হ্যাকিংয়ের কোনো ঘটনা ঘটেনি।

মার্কিন ফেডারেল রিজার্ভের সরল প্রতিক্রিয়া ছিল–চুরির সময় ইস্যুকৃত সমস্ত অর্থ স্থানান্তর অনুরোধ সুইফট নির্ধারিত প্রয়োজনীয় নিরাপত্তা প্রটোকল মেনেই করা হয়েছে। সুইফটের প্রধান নির্বাহী গটফ্রিড লিবিব্রান্ট একই কথা বলেন। যুক্তির খাতিরে ধরে নেওয়া যাক, হ্যাকাররা সুইফট বা ফেডারেল রিজার্ভের নেটওয়ার্কে ঢুকতে পেরেছিল। তা-ই যদি হয়, তাদের লক্ষ্য শুধুমাত্র বাংলাদেশের অ্যাকাউন্ট হলো কেন? আরো বেশি অর্থের আরো অনেক অ্যাকাউন্ট তো আছে। সুইফটের নেটওয়ার্ক ভাঙার মানে হচ্ছে বিশ্বজুড়ে অর্থ স্থানান্তর ব্যবস্থায় বিশাল ধস নামানো। আগেই ব্যাখ্যা করা হয়েছে, সুইফটের ডিজিটাল সার্টিফিকেট ভাঙা অসম্ভব না হলেও দুর্লজ্ঘ্য। যদি সত্যিই হ্যাক হতো, বিশ্বজুড়ে প্রযুক্তি প্রকাশনা ও সাইবার নিরাপত্তা দুনিয়ার শিরোনাম হতো সেটি। মজার ব্যাপার হলো, শুধুমাত্র একটি শীর্ষ প্রযুক্তি পত্রিকা ওয়ারড ম্যাগাজিনে একটিমাত্র প্যারায় মূলধারার অন্য একটি পত্রিকা গার্ডিয়ানের বরাত দিয়ে লুটপাটের খবর বেরিয়েছে। এতেই বোঝা যায়, খবরটির প্রযুক্তিগত গুরুত্ব কত গৌণ। অন্যান্য প্রযুক্তি প্রকাশনারও কোনো আগ্রহ চোখে পড়েনি।

অর্থনৈতিক প্রতিষ্ঠানগুলো ভাঙা অত্যন্ত কঠিন। ২০১৪ সালে ফেডারেল রিজার্ভে সর্বশেষ হ্যাকিংয়ের ঘটনা ঘটে। লরি লাভ নামের এক ব্রিটিশ নাগরিক 'এসকিউএল ইনজেকশন' প্রযুক্তি ব্যবহার করে ফেডারেল রিজার্ভের ব্যক্তিগত ডাটাবেজ হ্যাক করেন। এটি ওয়েবসাইট ও ডাটাবেজগুলোর অন্তর্নিহিত একটি দুর্বলতা এবং সহজেই সংস্কারযোগ্য; যদিও পুরোপুরি ত্রুটিমুক্ত নয়। তবে সেই হ্যাকার ফেডের অর্থনৈতিক ডাটায় ঢুকতে পারেননি। পাঁচ বছর আগে উইকিলিকস ও জুলিয়ান অ্যাসাঞ্জের বিরুদ্ধে মার্কিন সরকার নিষেধাজ্ঞা জারি করেছিল। কিভাবে? বড় বড় ক্রেডিট কার্ড কোম্পানি ও আর্থিক প্রতিষ্ঠানে মার্কিন সরকার চিঠি লিখে জানিয়ে দেয়, যাতে তাদের গ্রাহকরা উইকিলিকসের অ্যাকাউন্টে কোনো অর্থ জমা দিতে না পারে। উইকিলিকসের পক্ষে দাঁড়ানো বিশ্বের সবচেয়ে বড় হ্যাকিং কমিউনিটি অ্যানোনিমাস এরই প্রতিশোধ নেয়। অ্যানোনিমাসের এ প্রতিশোধ ছিল নিতান্তই মৃদু–একটি ডিসট্রিবিউটেড ডিনাইয়াল অব সার্ভিস (ডিডিওএস) অ্যাটাক। ডিডিওএস অ্যাটাক হলো ধারণক্ষমতার অতিরিক্ত রিকোয়েস্ট পাঠানোর মাধ্যমে সার্ভার স্বয়ংক্রিয়ভাবে বন্ধ করে দেওয়া। ডিডিওএস অ্যাটাক করে কোনো ডাটা চুরি বা কোনো বিশেষ ক্ষতি সাধন করা যায় না; উদ্দিষ্ট প্রতিষ্ঠানের সাময়িক অসুবিধার সৃষ্টি করা যায় মাত্র।

মার্কিন সামরিক বাহিনীতে সবচেয়ে বড় হ্যাকিংয়ের ঘটনা ঘটে ২০০২ সালে ব্রিটন গ্যারি ম্যাককিননের মাধ্যমে। তাঁর পদ্ধতি ছিল খুব সাধারণ; আজকের যুগের বিবেচনায় এটাকে হ্যাকিং না-ও বলা যেতে পারে। ম্যাককিননের নিজের স্বীকারোক্তি অনুযায়ী, তিনি শুধুমাত্র যেসব ব্যবহারকারী ব্যাংক পাসওয়ার্ড ব্যবহার করেন বা কোনো পাসওয়ার্ড ব্যবহার করেন না, তাঁদের খুঁজে মার্কিন সামরিক বাহিনীর কম্পিউটার নেটওয়ার্ক ভাঙতে সক্ষম হন। একেবারে অপটু হাতের কাজ। প্রায় একই সময়ে এক কিশোর একটি ফোন কোম্পানির টেকনিশিয়ানের ভেক ধরে সিআইএর পরিচালক ব্রেনানের ই-মেইল অ্যাকাউন্ট হ্যাক করে–ব্রেনান সেই কোম্পানির একজন গ্রাহক ছিলেন। এবং অবাক ব্যাপার হলো, ভেকধারী কোনোভাবে ফোন কোম্পানির এক চাকুরের পরিচয়পত্রও জোগাড় করেছিল–শুধুমাত্র ভেতর থেকে কেউ তথ্য ফাঁস করে দিলেই এটা সম্ভব। একবার পরিচালকের ফোনের ব্যক্তিগত শনাক্তকরণ নম্বর বা পিন ও অন্যান্য গুরুত্বপূর্ণ তথ্য হাতে চলে এলে ই-মেইল অ্যাকাউন্ট হ্যাক করা খুবই সহজ ছিল।

আরেকটি হাস্যকর ঘটনা হলো ২০১৪-এর শেষ দিকে সনি পিকচার্স হ্যাকিংয়ের ঘটনা। হ্যাকিং যখন হলো, সব দোষ দেওয়া শুরু হলো উত্তর কোরিয়ার ওপর, কারণ সনির সে সময় উত্তর কোরীয় নেতাকে ব্যঙ্গ করে বানানো ছবি মুক্তি দেওয়ার কথা ছিল। এফবিআই, সাথে হোয়াইট হাউসও উত্তর কোরিয়াকে দোষারোপ করল–স্বভাবতই ওয়াশিংটন প্রশাসনের রাজনৈতিক স্বার্থে। নিরাপত্তা বিশেষজ্ঞরা পরে তদন্ত করতে গিয়ে দেখলেন, এই ঘটনার সাথে উত্তর কোরিয়ার কোনো শক্ত যোগসূত্রই নেই। নর্স করপোরেশন নামে সিলিকন ভ্যালির অন্যতম শীর্ষ সাইবার নিরাপত্তা প্রতিষ্ঠান এই হ্যাকিংয়ের পেছনে সনির সাবেক ছয় কর্মকর্তার যোগসূত্র খুঁজে বের করল। এবং এখন পর্যন্ত এটিই হ্যাকিংয়ের সবচেয়ে বিশ্বাসযোগ্য কারণ, যদিও আইনিভাবে তা এখনো প্রমাণিত হয়নি। পরিশেষে নাতাঞ্জে ইরানের নিউক্লিয়ার স্থাপনার কম্পিউটারে স্টাক্সনেট ভাইরাস ঢুকিয়ে দেওয়ার কথা বলতে হয়, সে ভাইরাস ইন্টারনেট হয়ে আসেনি; কারণ স্থাপনাটি ছিল ইন্টারনেটমুক্ত এলাকা। বরং অভিযোগ আছে যে ইরান যন্ত্রাংশ কেনার আগে পশ্চিমা গোয়েন্দারা নির্মাণকারী প্রতিষ্ঠান সিমেন্সের সাথে যোগসাজশে এই ভাইরাস ঢুকিয়ে দেয়। মূলকথা হলো, হ্যাকিং কোনো সহজ ব্যাপার নয় বা শুধুমাত্র প্রযুক্তি দিয়েই করা যায় না। সেখানে অবশ্যই মনুষ্য হস্তক্ষেপের প্রয়োজন পড়ে অথবা গ্যারি ম্যাককিননের ক্ষেত্রে যেমন দেখলাম অর্থাৎ সিস্টেমে যথেষ্ট গুরুতর নিরাপত্তা ত্রুটি থাকতে হবে।

একাধিক কারণে এটিকে নিছক নিরাপত্তা দুর্বলতাজনিত হ্যাকিং মনে করাটা কঠিন। আমরা এখন জানি যে অপরাধীরা সম্ভাব্য সকল নিরাপত্তা চেকিং পেরিয়ে সিস্টেমে ঢুকতে পেরেছিল। একই সাথে আমরা যদি প্রথম পাঁচটি লেনদেন ও সংশ্লিষ্ট অর্থ পরিশোধ নির্দেশনাগুলো খেয়াল করি, তাহলে পরিষ্কার বোঝা যাবে যে কাজটি ভেতর থেকে কেউ করেছে।

বাংলাদেশ ব্যাংক লুটপাটের ঘটনায় ফেরা যাক। একাধিক কারণে এটিকে নিছক নিরাপত্তা দুর্বলতাজনিত হ্যাকিং মনে করাটা কঠিন। আমরা এখন জানি যে অপরাধীরা সম্ভাব্য সকল নিরাপত্তা চেকিং পেরিয়ে সিস্টেমে ঢুকতে পেরেছিল। একই সাথে আমরা যদি প্রথম পাঁচটি লেনদেন ও সংশ্লিষ্ট অর্থ পরিশোধ নির্দেশনাগুলো খেয়াল করি, তাহলে পরিষ্কার বোঝা যাবে যে কাজটি ভেতর থেকে কেউ করেছে। ঢাকা ট্রিবিউনের প্রতিবেদন অনুযায়ী অর্থ পরিশোধ নির্দেশনাগুলো ছিল :

* কাঁচপুর, মেঘনা ও গোমতী দ্বিতীয় সেতু নির্মাণ প্রকল্প
* ঢাকা মাস র‍্যাপিড ট্রান্সপোর্ট ডেভেলপমেন্ট প্রজেক্টের নামে জাইকার ঋণ
* আইপিএফএফ প্রজেক্ট সেলের কনসালটেন্সি ফি
* ভেড়ামারা কম্বাইন্ড সাইকেল পাওয়ার প্লান্ট ডেভেলপমেন্ট প্রজেক্টের ইঞ্জিনিয়ারিং কন্সালটেন্সি ফি

প্রতিটি পেমেন্ট অর্ডার বৈধ এবং প্রতিটির বাস্তব অস্তিত্ব আছে। আরো উল্লেখ করা দরকার যে দৈনিক পত্রিকায় এই প্রজেক্টগুলোর খবর খুঁজে পাওয়া যায় না। এর মানে হলো, বাংলাদেশ ব্যাংকের

কাজের ধারা এবং দেশের চলমান উন্নয়ন প্রকল্প বিষয়ে অপরাধীদের বিচক্ষণ ধারণা আছে। অধিকন্তু এদেশে কিছুকাল ধরে বাস না করে কোনো বিদেশির পক্ষে এদেশীয় নাম ব্যবহার করে পেমেন্ট নির্দেশনা পাঠানো খুব অস্বাভাবিক ব্যাপার। দ্বিতীয়ত, সব সিকিউরিটি চেকিং পেরিয়ে আসার মানে হলো, অপরাধীদের বাংলাদেশ ব্যাংকের প্রাইভেট কি ও ডিজিটাল সার্টিফিকেটে প্রবেশাধিকার ছিল। নিরাপত্তা প্রতিষ্ঠান আরএসএর জ্যেষ্ঠ পরিচালক কায়ভান আলিকানি একই কথা বলেছেন। আরএসএ পৃথিবীর অধিকাংশ বড় ব্যাংকের সাইবার নিরাপত্তা প্রদান করে। এখন পর্যন্ত সার্টিফিকেট ফাঁস হয়ে যাওয়ার কোনো কারণ কেউ দেখাতে পারেননি। হ্যাকাররা দূরে থেকে ডিজিটাল সার্টিফিকেট কপি করবে, এটা অসম্ভব। ডিজিটাল সার্টিফিকেট কম্পিউটারের সবচেয়ে নিরাপদ জায়গায় রাখা হয় এবং শুধুমাত্র অ্যাডমিনিস্ট্রেটরের সেখানে প্রবেশাধিকার আছে। তাছাড়া থ্রিএসকি ডিভাইস ব্যবহার করা হলে মোটামুটি নিশ্চিতভাবে বলা যায় যে বাংলাদেশ ব্যাংকের উর্ধ্বতন কর্তৃপক্ষের জ্ঞাতসারে এই লুটপাট করা হয়েছে। এসব যেকোনো ক্ষেত্রেই ব্যাংকের কর্মকর্তাদের জড়িত থাকার সম্ভাবনা অনেক বেশি।

লুটপাটের পরে বাংলাদেশ ব্যাংক, ওয়াল স্ট্রিট জার্নালের রিপোর্ট অনুযায়ী, সিলিকন ভ্যালি ভিত্তিক প্রতিষ্ঠান ফায়ারআইকে নিয়োগ করে। তাদের কাজ ছিল লুটপাট কিভাবে হলো সেটা খুঁজে বের করা এবং তারা সিদ্ধান্ত দেয় যে বাংলাদেশ ব্যাংকের কম্পিউটার সিস্টেমে ম্যালওয়্যার ইনস্টল করা ছিল। ফায়ারআইয়ের দাবি অনুযায়ী এক ধরনের কি লগিং সফটওয়্যার ইনস্টল করা ছিল। এটির কাজ হলো কোনো কম্পিউটারের কি-বোর্ডের যাবতীয় চাপ রেকর্ড করা এবং হ্যাকারকে পাঠিয়ে দেওয়া। এই দাবি মেনে নিলেও এটা পরিষ্কার হয় নয় যে হ্যাকাররা ডিজিটাল সার্টিফিকেটে কিভাবে ঢুকল এবং থ্রিএসকি ডিভাইস ব্যবহার করা হয়েছিল কি না। সনি পিকচার্সের নিজস্ব হ্যাকিংয়ের সময় যাদের নিয়োগ করা হয়েছিল, ফায়ারআই হলো সেই কোম্পানি এবং কোনো নির্দিষ্ট তথ্য-প্রমাণ দিতে না পারলেও তারা সেই ঘটনায় উত্তর কোরিয়াকে দায়ী করেছিল। আর ম্যালওয়্যারও একা একা ইনস্টল হতে পারে না, ইচ্ছায় হোক বা অনিচ্ছায়, কোনো ব্যক্তিকে লাগে। বাজারের সর্বশেষ এবং সম্ভবত সবচেয়ে ভয়ানক ম্যালওয়্যার হলো র‍্যানসোমওয়্যার –সেটিও একা একা ইনস্টল হতে পারে না, কম্পিউটারের প্রি-ইনস্টলড সফটওয়্যার লাগে।

সম্প্রতি আমরা জানতে পারি সিআইডির দেয়া তথ্য অনুসারে ত্রুটিপূর্ন নেটওয়ার্কিং ডিভাইস ব্যাবহারের জন্য হ্যাকিং হয়েছে। যদি ধরেও নিই কোথাও ত্রুটিপূর্ণ নেটওয়ার্কিং ডিভাইস ব্যাবহার হয়েছে এবং ফায়ারওয়াল ছিল না বলে ম্যালওয়্যার ট্র্যান্সমিট হয়েছে তারপরও প্রশ্ন থেকে যায়। প্রথমত, কি ধরনের ম্যালওয়্যার প্রবেশ করলো এবং কিভাবে? ফায়ারওয়ালের একমাত্র কাজ হচ্ছে ম্যালওয়্যার ঢুকতে বাধা দেয়া। ম্যালওয়্যার ঢোকার পরে তা কাজ করতে ডিজিটাল সার্টিফিকেট প্রয়োজন। এই ডিজিটাল সার্টিফিকেট কি করে চুরি হল? ডিজিটাল সার্টিফিকেট কমপিউটারের অত্যন্ড় গোপনীয় স্থানে রাখা হয় এবং তা জানতে শুধুমাত্র এডমিনিস্ট্রিটেটিভ মোডের মাধ্যমে প্রবেশ করতে হয়। যদি ধরে নিই "তথাকথিত ম্যালওয়্যার" কোনভাবে ডিজিটাল সার্টিফিকেটও চুরি করতে সক্ষম হয়েছে তারপরও প্রশ্ন থেকে যায়। পাসওয়ার্ড বা থ্রিএসকি ডিভাইস(3SKey device)কিভাবে চুরি হল? আমরা নেটওয়ার্কিং ডিভাইস এবং অপ্রতুল সিকিউরিটি প্র্যাকটিসের অযুহাত দেখিয়ে দোষীর অন্যান্য অনেক ভূমিকাকে অস্বীকার করছি। আর এই সুযোগে সিকিউরিটি ইন্ডাস্ট্রিগুলিকে নতুন নতুন ব্যাবসার সুযোগ হাতে তুলে দিচ্ছি।

ম্যালওয়্যারের যুক্তি করা একভাবে বেশ লাভজনক, মানুষ এ নিয়ে তখন আর বেশি মাথা ঘামায় না। আইনি সুবিধাও আছে–কারণ কেউ জানে না কে এটি ইনস্টল করেছে; ফলে কারো দিকে অভিযোগের আঙুল ওঠে না। এ ঘটনায় বাংলাদেশের মিডিয়া ও ব্যাংকগুলোর প্রতিক্রিয়া আমরা দেখেছি, সবাই আরো বেশি সাইবার নিরাপত্তার কথা বলছেন। এ ধরনের যুক্তি বাংলাদেশের সরকারি ও বেসরকারি উভয় ধরনের প্রতিষ্ঠানকে তথাকথিত সর্বাধুনিক প্রযুক্তির আড়ালে কুখ্যাত নিরাপত্তা যন্ত্রাংশ সংযুক্ত করে আরো অধিক টাকা বানানোর সুযোগ ও প্রণোদনা দেয়। কোনো দিন যদি আমরা জানতে পারি যে এই লুটপাটের ঘটনা শীর্ষ পর্যায়ের জ্ঞাতসারে ব্যাংকের ভেতর থেকেই হয়েছে, সেটি অবাক করার মতো ব্যাপার হবে না। কারণ মাত্র কয়েক দিন আগে ফাঁস হওয়া পানামা পেপারসে দেখি, ধনী বাংলাদেশিরা ব্রিটিশ ভার্জিন আইল্যান্ডের মতো কর ফাঁকির স্বর্গরাজ্যে অফশোর অ্যাকাউন্ট খুলেছে। আর বাংলাদেশ ব্যাংকের এ বিষয়ে আগে থেকে না জানার সম্ভাবনা খুব কম।

***তারিফ রিয়াদ রহমান:*** প্রভাষক, নর্থ সাউথ বিশ্ববিদ্যালয়
***ইমেইল:*** tarifspeaks@gmail.com

[তারিফ রিয়াদ রহমানের Bangladesh Bank Scandal: The Heist, Hype and Hilarity শীর্ষক লেখাটি সর্বজনকথা'র জন্য অনুবাদ করেছেন ***তন্ময় কর্মকার***]

## টীকা

১) বাংলাদেশ রেমিট্যান্স, রপ্তানি এবং ইত্যাদি থেকে প্রাপ্ত ডলার মার্কিন কেন্দ্রীয় ব্যাংক বা ফেডারেল রিজার্ভের তত্ত্বাবধানে চলতি অ্যাকাউন্টে জমা রাখে। যেকোনো আমদানি এই অ্যাকাউন্টের মাধ্যমে পরিশোধিত হয়। বাংলাদেশ ছাড়াও আরো অনেক দেশ ও জাতির ডলার রিজার্ভ ফেডারেল রিজার্ভের তত্ত্বাবধানে আছে।

২) সংশ্লিষ্ট চারজন ফিলিপিনো হলেন এনরিকো থিওডর ভাস্কুয়েজ, আলফ্রেড স্যান্টোস ফারগারা, মাইকেল ফ্রান্সিসকো ক্রুজ ও জেসি ক্রিস্টোফার লাগরোসাস।

৩) জাংকেট অপারেটর হলো কোনো ব্যক্তি বা প্রতিষ্ঠান, যে বা যারা তাদের ক্যাসিনোতে জুয়া খেলার একান্ত উদ্দেশ্যে ও সুবিধার্থে গ্রাহক বা পর্যটকদের থাকা-খাওয়া ও যাতায়াতের সুবন্দোবস্ত করে।

৪) সুইফট বা Society for Worldwide Interbank Financial Telecommunication হলো ব্যাংকিং যোগাযোগের প্রয়োজনে অর্থনৈতিক লেনদেন সংক্রান্ত একটি আদর্শ কমিউনিকেশন প্রটোকল। তবে অবশ্যই জেনে রাখা দরকার যে সুইফট বা SWIFT কোনো অর্থনৈতিক প্রতিষ্ঠান নয়, অথবা এটি নিজে বা কারো পক্ষে কোনো অর্থনৈতিক লেনদেন করে না; বরং উপরোক্ত প্রতিষ্ঠানগুলোর মধ্যে যোগাযোগ সমন্বয়ের কাজ করে মাত্র।

**তথ্যসূত্র:**

1. Lucas. L Daxim, 29th February 2016. $100-M laundering via PH banks, casinos probed. http://business.inquirer.net /207742/ 100-m-laundering-via-ph-banks-casinos-probed

2. Anatomy of a Bank Robbery, 11th March 2016. http://www.dhakatribune.com/bangladesh

/2016/mar/11/anatomy-bank-robbery
3. RCBC allows $81m BB fund withdrawal despite stop order, 16th March 2016. http://newagebd.net/211867/rcbc-allows-81m-bb-fund-withdrawal-despite-stop-order/

4. Hacker's spelling slip foils billion-dollar bank heist, 10th March 2016. http://www.dw.com/en/hackers-spelling-slip-foils-billion-dollar-bank-heist/a-19106343

5. Samath Feizal, 13th March 2016. Sri Lankan teller helps bust world's biggest bank fraud. http://www.sundaytimes.lk /160313 /news /sri-lankan-teller-helps-bust-worlds-biggest-bank-fraud-186459.html

6. Spelling mistake prevented hackers taking $1bn in bank heist, 10th March 2016. http://www.theguardian.com /business/2016/mar/10/spelling-mistake-prevented-bank-heist

7. Lema Karen, 15th March 2016. Cash from Bangladesh bank hack in Manila. http://www.news.com.au/finance/business /breaking-news/cash-from-bangladesh-bank-hack-in-manila/news-story/19a8d426ac581af12a0fb38e26c6064d

8. Wong surrenders $4.6m of BB money to Filipino authorities, 31st March 2016. http://newagebd.net/216471/wong-surrenders-4-6m-of-bb-money-to-filipino-authorities/

9. International Migration at All-Time High, 15th December 2015. http://www.worldbank.org/en/news/press-release/2015/12/18/international-migrants-and-remittances-continue-to-grow-as-people-search-for-better-opportunities-new-report-finds

10. Senate probes $81-M money laundering, 16th March 2016. http://www.mb.com.ph/senate-probes-81-m-money-laundering/

11. SWIFT – About Us. https://www.swift.com/about-us

12. SWIFT – 3SKey. https://www.swift.com/our-solutions/3skey

13. Walker Lindsay, 28th August 2015. Information: What is a Digital Certificate?. https://wikis.utexas.edu/pages/ viewpage.action?pageId=112331926

14. The Hardness of Factoring. http://www.cs.virginia.edu/~kam6zx/is-it-secure/the-hardness-of-factoring/

15. Ohmart Paul. RSA Encryption Key Size Requirements Change in 2011. http://web.townsendsecurity.com/bid /23970/RSA-Encryption-Key-Size-Requirements-Change-in-2011

16. 3SKey for Corporates [online pdf document]. October 2012. https://www.swift.com/node/14791

17. Federal Reserve denies Bangladesh Bank's US account hacked, money stolen, 8th March 2016. http://bdnews24.com/economy/2016/03/08/federal-reserve-denies-bangladesh-banks-us-account-hacked-money-stolen

18. Security News This Week: Hackers Spoil Their $1 Billion Bank Heist With a Typo. 12Th March 2016. http://www.wired.com/2016/03/security-news-week-hackers-spoil-1-billion-bank-heist-typo/

19. Stempel Jonathan. 27Th February 2014. British man charged with hacking Federal Reserve computers. http://www.reuters.com/article/us-usa-crime-hacking-idUSBREA1Q1R720140227

20. Gillmour, Dan. 27Th October 2011. WikiLeaks payments blockade sets dangerous precedent. http://www.theguardian.com/commentisfree/cifamerica/2011/oct/27/wikileaks-payments-blockade-dangerous-precedent

21. McMillan Robert. 28Th January 2011. FBI joins Met in 'Anonymous' crackdown. http://www.computerworlduk.com /news/security /fbi-joins-met-in-anonymous-crackdown-3258467/

22. Hacker fears 'UFO cover-up'. 5Th May 2006. http://news.bbc.co.uk/2/hi/programmes/click_online/4977134.stm

23. Zetter Kim. 19Th October 2015. Teen Who Hacked CIA Director's Email Tells How He Did It. http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

24. Zetter Kim. 17Th December 2014. The Evidence That North Korea Hacked Sony Is Flimsy. http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

25. Post Staff Reporter. 30Th December 2014. New evidence Sony hack was 'inside' job, not North Korea. http://nypost.com/2014/12/30/new-evidence-sony-hack-was-inside-job-cyber-experts/

26. Zetter Kim. 11Th March 2014. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

27. Finkle Jim. 9Th March 2016. Criminals in Bangladesh heist likely studied bank's inner workings. http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0WB2PI

28. Al-Mahmood Zain Syed. 22Nd March 2016. Hackers Lurked in Bangladesh Central Bank's Servers for Weeks. http://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678.

29. Barrett Brian. 7Th March 2016. Hack Brief: Ransomware Strikes Apple's OS X for the First Time. http://www.wired.com/2016/03/hack-brief-ransomware-hits-mac-os-x-first-time/

30. International Consortium of Investigative Journalists(ICIJ) – Panama Papers. https://panamapapers.icij.org/

31. পানামা পেপারস: অর্থ পাচারের তালিকায় ২৫ বাংলাদেশি, ৬ এপ্রিল, ২০১৬. http://goo.gl/VOQtpw.

32. Kirk Jeremy. 9Th September 2016. North Korea is likely behind attacks exploiting a Korean word processing program. http://www.pcworld.com/article/2982577/north-korea-is-likely-behind-attacks-exploiting-a-korean-word-processing-program.html