Penggunaan Kriptografi Kunci Publik untuk Mekanisme *Forgot Password*

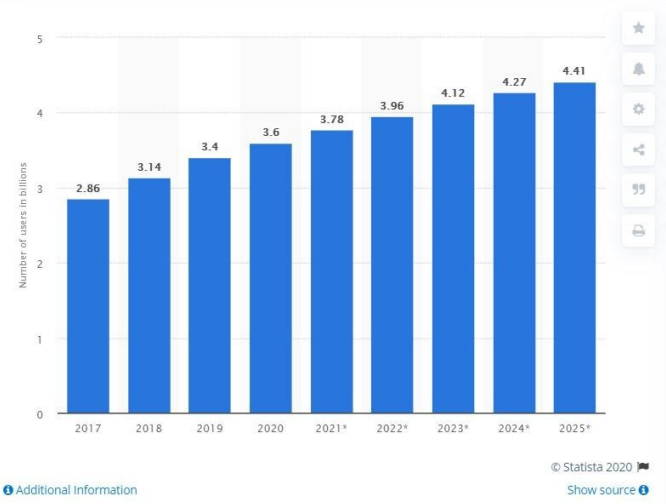
Muhammad Al Terra 13517145
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*author@itb.ac.id*

Abstract*—Penggunaan media sosial di era modern ini berarti adalah penggunaan internet sudah mencapai ke ranah pribadi orang-orang. Banyak sekali hal-hal yang berkaitan dengan hal-hal privat sudah diletakkan di profil media sosial, seperti foto, pembicaraan-pembicaraan intim dan hal-hal semacamnya. Semakin canggihnya teknologi berarti semakin canggih pula metode untuk mendapatkan informasi dengan cara-cara yang sifatnya ilegal, metode-metode *social engineering* atau peretasan dapat membahayakan informasi setiap orang. Selain itu, ada dampak pula dari jumlah media sosial yang banyak, yaitu banyaknya kata sandi yang harus diingat. Diusulkan di makalah ini suatu metode untuk mempermudah mekanisme *forgot password.

***Keywords*—Password, Kriptografi, Kunci, Publik, Privat**

I. Introduction

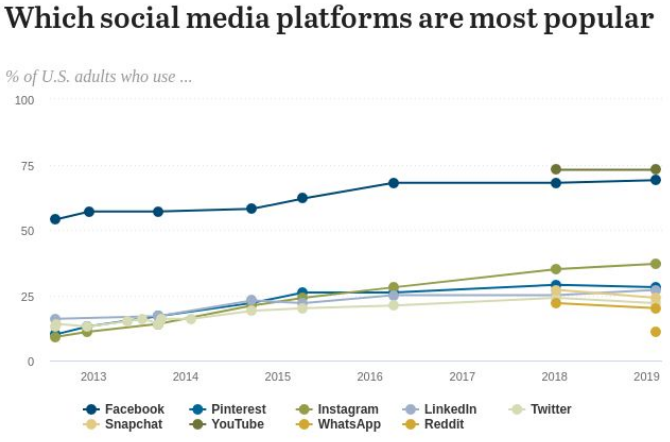
Di era modern ini banyak sekali pengguna internet dan penggunaan identitas-identitas digital seperti media sosial. Penggunaan media sosial ini dilakukan oleh berbagai kalangan tidak memandang tingkat pendidikan yang mereka miliki. Prediksi penggunaan media sosial akan terus bertambah seperti yang diperlihatkan di grafik berikut (Statista, 2020):



Peningkatan penggunaan internet untuk demografi usia di bawah 18 dan diatas 44 tahun akan memunculkan kekhawatiran bahwa pengguna internet tersebut tidak memahami bagaimana cara kerja media sosial yang ada di dunia maya dan bahaya-bahaya yang dapat menghampiri mereka. Koobface merupakan salah satu serangan yang dapat diluncurkan untuk mentarget pengguna media sosial yang tidak tahu-menahu mengenai keamanan informasi serta aktor-aktor jahat yang berada di dunia *online*.

Menurut Kaspersky Koobface telah merugikan masyarakat digital cukup banyak sehingga apabila dikumulatifkan maka kerugian akan mencapai 66.4 juta dolar (Kaspersky, 2020). Mekanisme Koobface menggunakan teknik *social engineering*, yaitu adalah suatu teknik penipuan agar pihak yang ditipu dapat menyampaikan informasi pribadi miliknya, strategi utama dari social engineering adalah untuk memanfaatkan emosi dan reaksi alamiah targetnya (Norton, 2018).

Hal ini memunculkan permasalahan karena emosi orang-orang bukanlah suatu hal yang mudah untuk dikendalikan. Ketidakpastian emosi dan perasaan yang dapat dimanfaatkan Koobface memungkinkan pihak-pihak yang, walaupun telah memahami betul mengenai adanya social engineering dan teknik-teknik untuk menghindarinya, untuk jatuh ke skema penipuan tersebut. Permasalahan lain yang dihadapi oleh masyarakat digital pada era modern ini adalah banyaknya aplikasi media sosial dan aplikasi-aplikasi yang membutuhkan otentikasi. Tercatat pada tahun 2011 ada 9 media sosial yang populer yang digunakan oleh orang-orang amerika dengan distribusi lebih tinggi di Facebook dan YouTube, namun persentase yang relatif sama di 7 media sosial yang lain (Pew Research, 2019) :



Menyadari angka yang tinggi dari penggunaan media sosial

ini maka permasalahan kedua dapat dirumuskan yaitu, banyaknya dan fenomena lupa password yang semakin sering dialami. Makalah ini mencoba untuk mengusulkan potensial alternatif solusi untuk menyelesaikan permasalahan reset password. Dengan menggunakan kriptografi kunci publik, maka diharapkan bahwa metode ini dapat mengurangi resiko bocornya informasi yang menyeluruh. Contoh kasus yang dapat diatasi dengan kasus ini adalah apabila terdapat seorang peretas yang telah mendapatkan kredensial login untuk masuk ke suatu email seorang pengguna sosial media lalu mencoba untuk melakukan reset password ke akun sosial media yang terhubung ke email tersebut.

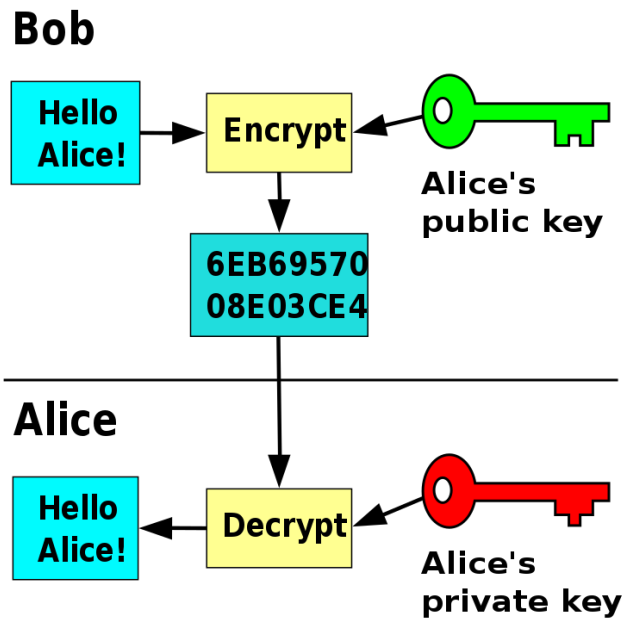
II. Algoritma Kunci Publik

Algoritma kunci publik adalah algoritma yang memiliki 2 kunci yang berbeda, kunci publik dan kunci privat. Kunci publik adalah kunci yang hanya dapat mengenkripsi pesan tetapi tidak dapat membuka pesan, sedangkan kunci privat adalah kunci yang bisa membuka pesan-pesan yang telah dienkripsi oleh kunci publik. Apabila diibaratkan sebagai kotak dan gembok lalu dimisalkan Alice dan Bob adalah pasangan yang akan mengirim pesan, maka Alice akan mengirim suatu kotak kosong yang didepannya ditambahkan suatu gembok yang belum dikencangkan. Saat Bob menerima kotak tersebut, Bob akan memasukkan pesan ke dalam kotak dan menekan gembok sehingga terkunci, lalu dikirimkan kembali ke Alice. Pemilik kunci yang bisa membuka kotak tersebut hanya Alice, sehingga walaupun kotak tersebut disadap atau dicuri orang. Orang-orang tidak dapat membaca isinya karena kunci milik Alice tidak pernah berada pada domain publik (Munir, 2020).

Ilustrasi kunci publik dalam bentuk gembok yang belum dikunci

Ilustrasi kunci privat dalam bentuk kunci yang bisa membuka gembok

Kunci publik pada analogi ini adalah kotak dan gembok yang dikirimkan oleh Alice, plaintext adalah pesan yang dimasukkan oleh Bob, ciphertext adalah kotak yang sudah digembok dan memiliki pesan dari Bob, kunci privat adalah kunci yang dimiliki Alice yang dapat membukanya.



Untuk menciptakan mekanisme tersebut dimanfaatkan persamaan matematika yang tidak mudah untuk dipecahkan, yaitu adalah persamaan matematika yang memiliki kompleksitas tinggi. Berikut adalah beberapa algoritma kunci publik beserta permasalahan matematika yang digunakannya.

1. Algoritma ElGamal, memanfaatkan kesulitan menghitung logaritma diskrit
2. Algoritma RSA, memanfaatkan kesulitan melakukan pencarian faktor prima
3. Algoritma ECC, memanfaatkan medan Galois

Kakas Cleopatra adalah kakas yang memiliki penggunaan algoritma RSA sebagai implementasi dari mekanisme kunci publik tersebut. Penggunaan Cleopatra juga relatif mudah digunakan oleh orang-orang awam. Oleh karena itu tidak menutup kemungkinan bahwa orang-orang pada masa yang akan datang akan memiliki kunci pribadi yang mereka gunakan untuk segala urusan.

Kemudahan dan seringnya penggunaan RSA akan menjadi salah satu alasan untuk digunakan algoritma tersebut. Algoritma ElGamal atau ECC yang memanfaatkan medan Galois juga bisa digunakan namun tidak akan dibahas mendalam.

III. Algoritma RSA

Algoritma RSA (Rivest-Shamir-Adleman) adalah salah satu algoritma kriptografi kunci publik yang implementasinya memanfaatkan kesulitan pencarian faktor-faktor prima dari suatu bilangan. Hal ini dapat dipahami secara intuitif jika diberikan suatu bilangan N yang merupakan produk dari 2 bilangan prima dan salah satunya bukan 1, maka akan dihasilkan suatu bilangan semiprima yang hanya memiliki 4 faktor, bilangan tersebut, 1, bilangan prima p yang tidak diketahui dan bilangan prima q yang tidak diketahui.

Untuk angka-angka dengan jumlah representasi bit yang

rendah akan memungkinkan untuk dipecah oleh sebuah komputer. Rekor yang tercatat adalah pemecahan RSA dengan representasi 768 bit dengan pendekatan Morrison-Brillhart, namun standar yang digunakan sekarang melebihi 2 kali lipat dari jumlah tersebut (2048). Munculnya komputer quantum bersamaan dengan algoritma Shor yang dapat menyelesaikan permasalahan faktorisasi dalam waktu log(n) akan menjadi permasalahan, namun komputer quantum masih belum ada yang dapat digunakan secara massal dan sedemikian rupa sehingga orang biasa bisa memilikinya, oleh karena itu algoritma RSA dianggap aman.

Ada beberapa variabel yang digunakan pada implementasi algoritma RSA (Munir, 2020).

1. p dan q bilangan prima (rahasia)
2. n = p q (tidak rahasia)
3. φ (n) = (p – 1)(q – 1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
   Syarat: PBB(e, (n)) = 1 , PBB = pembagi bersama terbesar = gcd
5. d (kunci dekripsi) (rahasia) d dihitung dari d e -1 mod ((n))
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Berikut adalah langkah pembangkitan kunci tersebut:

1. Pilih dua bilangan prima, p dan q
2. Hitung n = pq.
3. Hitung (n) = (p – 1)(q – 1).
4. Pilih sebuah bilangan bulat e sebagai kunci publik, e harus relatif prima terhadap (n).
5. Hitung kunci dekripsi, d, dengan persamaaan ed 1 (mod (n)) atau d e –1 mod ((n))

Ada pula langkah enkripsi sebagai berikut:

1. Nyatakan pesan menjadi blok-blok plainteks:
   m_1, m_2, m_3
   (Syarat: $0 \leq m_i < n - 1$)
2. Hitung blok cipherteks c_i untuk blok plainteks m_i menggunakan kunci publik e dengan persamaan $c_i = m_i^e \mod n$

Langkah dekripsi sebagai berikut:

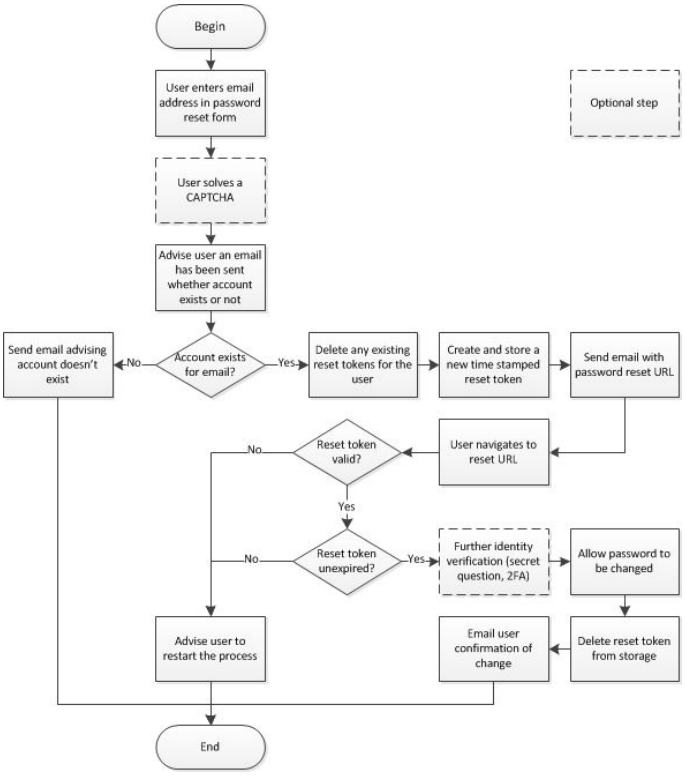
1. Nyatakan pesan menjadi blok-blok plainteks:
   c_1, c_2, c_3
   (Syarat: $0 \leq c_i < n - 1$)
2. Hitung blok cipherteks c_i untuk blok plainteks m_i menggunakan kunci publik e dengan persamaan $m_i = c_i^d \mod n$

Kakas Cleopatra adalah kakas yang memiliki penggunaan algoritma RSA sebagai implementasi dari mekanisme kunci publik tersebut. Penggunaan Cleopatra juga relatif mudah digunakan oleh orang-orang awam. Oleh karena itu tidak menutup kemungkinan bahwa orang-orang pada masa yang akan datang akan memiliki kunci pribadi yang mereka gunakan untuk segala urusan.

IV. Mekanisme Penyimpanan Password

Hampir semua media sosial yang digunakan oleh orang-orang pada era modern ini menggunakan setidaknya single factor authentication yang melibatkan password. Kata sandi yang digunakan ini adalah kata yang bersifat personal, rahasia dan tidak boleh bocor bahkan oleh orang-orang yang menyimpan password tersebut, seperti administrator database. Hal ini penting dilakukan karena sekitar 85% pengguna media sosial yang banyak ini melakukan password reusing (Abbott, 2018), hal ini berarti apabila password tersebut disimpan dalam bentuk *plain text* maka, apabila basis data bocor atau administrator basis data memiliki niatan yang buruk maka password tersebut akan tersedia tanpa ada perlindungan. Strategi yang biasa diimplementasikan untuk mengatasi kasus ini adalah melakukan hashing password baik dengan SHA 1, MD5, atau SHA 2 (Kioon, 2013). Namun metode seperti itu memunculkan masalah saat user yang benar-benar adalah pemilik dari akun lupa password dan ingin masuk ke akun.

Mekanisme yang standar digunakan untuk melakukan reset password dapat meliputi beberapa langkah umum sebagai berikut:



Namun permasalahan akan muncul kembali apabila fitur-fitur yang ditawarkan memiliki permasalahan contohnya untuk email, apabila seorang peretas memiliki akses ke email, maka hacker tersebut dapat meminta *reset password* yang diarahkan ke email yang sudah dikuasai oleh penyerang. Usulan solusi ini akan diharapkan untuk mengurangi resiko bocornya semua akun yang terhubung ke 1 email yang sama

dengan mengandalkan kriptografi kunci publik, sehingga user mengunggah kunci publik yang bisa dibuka dengan kunci privat mereka lalu situs melakukan enkripsi terhadap password plaintext tersebut dan menyimpannya di basis data. Sehingga menu *forgot password* yang awalnya mengarahkan user untuk mengecek email dapat menjadi pengingat password yang apabila diklik akan mengunduh file password dalam bentuk ciphertext yang hanya bisa dibuka oleh kunci user.

V. Fungsi Hash

Fungsi hash pada dasarnya adalah fungsi yang dapat menerima input berukuran apapun dan memetakannya ke output yang berukuran pasti. Input tidak mempengaruhi ukuran output yang keluar, baik input tersebut adalah 1 karakter seperti huruf 'A' dan seisi novel Lord of the Rings maka outputnya akan berukuran sama. Fungsi hash merupakan fungsi yang tidak bersifat reversible, beda dengan fungsi enkripsi, fungsi hash tidak memungkinkan untuk mengambil plaintext atau teks awal yang dimasukkan ke fungsi untuk menghasilkan output tersebut. Beberapa fungsi hash yang populer digunakan adalah (Munir, 2020):

1. MD5
2. SHA-1
3. SHA-256
4. SHA-512
5. SHA-3
6. Keccak

Fungsi hash biasa digunakan untuk menyimpan password pada basis data lalu dicocokkan dengan password yang sudah dikirim oleh user saat akan melakukan login. Pencocokan ini bukan melalui proses dekripsi teks yang disimpan di basis data dan membandingkan hasil keduanya, tetapi justru kata sandi yang sifatnya plaintext tersebut dihash dan dibandingkan nilai hashnya.

Permasalahan yang muncul pada masa modern ini adalah tingginya kemungkinan seseorang untuk lupa akan password. Fungsi hash yang bersifat tidak reversible berarti pengguna tidak bisa menanyakan password aslinya apa ke siapapun dan hanya bisa mencoba untuk menanya kepada dirinya password dulunya apa. Hal ini ditanggulangi dengan utilitas reset password yang biasanya mengirimkan pesan atau kode pada email pengguna atau nomor ponsel yang dapat dimasukkan.

Pendekatan ini membuka celah apabila, email yang sudah dikuasai oleh peretas pada suatu waktu digunakan untuk melakukan *reset password* terhadap semua akun yang terhubung dengan akun pengguna email tersebut.

Bukan berarti fungsi hash seharusnya tidak digunakan, fungsi hash adalah alternatif yang murah yang tidak membutuhkan sumber daya komputasi yang besar untuk melakukan hashing dan perbandingannya, serta orang-orang yang ingin membobol suatu website dengan menyadap hash yang dimiliki oleh seseorang akan cenderung memiliki *Return on Investment* yang jauh lebih rendah dibanding cara lainnya, melainkan usaha komputasi dan hal-hal lain akan jauh lebih mahal dari isi akun tersebut. Teknik ini juga dapat digunakan sebagai salah satu cara untuk menambah cara otentikasi, selain dengan nomor HP, email dan hal-hal semacamnya, upload digital signature yang dibuat atas private key yang dimiliki oleh pengguna akan menutup kemungkinan orang lain memalsukan dirinya sebagai pengguna.

VI. Usulan Solusi

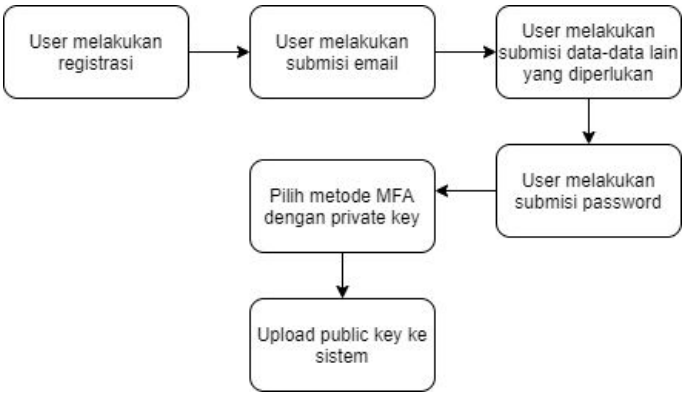
Solusi yang ditawarkan berbentuk sebagai salah satu bentuk kemudahan yang memiliki derajat keamanan yang cukup untuk menjadikan metode ini tidak membahayakan informasi yang dimiliki orang tersebut. Implementasi ini dibuat pula dengan asumsi bahwa kunci pribadi sudah diketahui oleh semua pihak dan sudah digunakan secara umum oleh orang-orang.

Hal ini bukanlah asumsi yang absurd atau tidak berlandasan, kesadaran akan keamanan informasi dan bagaimana pentingnya data milik diri sendiri terus berkembang, memang pada zaman sekarang usaha yang biasanya dilakukan untuk melakukan perlindungan atas data pribadi mereka masih hanya dalam bentuk password yang kuat dan menggunakan *software antivirus* (Al-Janabi, 2016), namun tidak menutup kemungkinan bahwa saat teknologi sudah semakin berkembang dan isu keamanan data akan menjadi lebih marak maka permasalahan cyber security akan menyerupai keamanan rumah dan ini senada dengan perubahan-perubahan yang dialami oleh manusia yang secara lambat laun telah berpindah menjadi netizen-netizen yang berada di internet. Dengan asumsi bahwa pemahaman masyarakat digital akan pentingnya memiliki kunci privat kriptografi sudah tinggi maka mekanisme ini dapat diimplementasikan.

Pada proses awal pendaftaran suatu akun pengguna di sosial media biasanya ada beberapa hal yang akan ditanyakan, diantaranya adalah *username*, *email* dan tentu saja password. Pada situs-situs yang lebih modern mereka akan menanyakan hal-hal yang sifatnya lebih intim atau pribadi seperti nomor HP atau nomor keamanan sosial.

Proses yang baru ini akan ditambah setelah password disubmit. Maka *website* akan memunculkan tahapan tambahan. Tahapan ini akan memberikan 2 pilihan pada pengguna media sosial, pilihan pertama adalah untuk meminta website untuk melakukan generasi pasangan *public key* dan *private key* yang random serta password yang sudah dienkripsi oleh *public key* yang selanjutnya disimpan di basis data. Pilihan kedua adalah untuk segera menerima public key yang sudah dimiliki oleh pengguna yang dapat bisa dibuka oleh *private key* di mesin lokal tersebut.

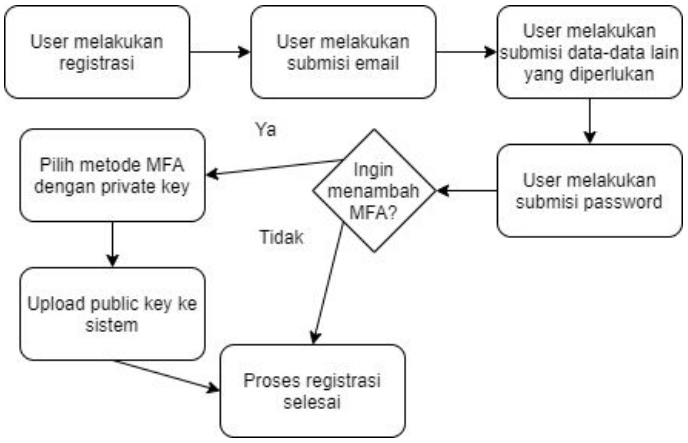
Berikut adalah gambaran langkah-langkah tersebut:



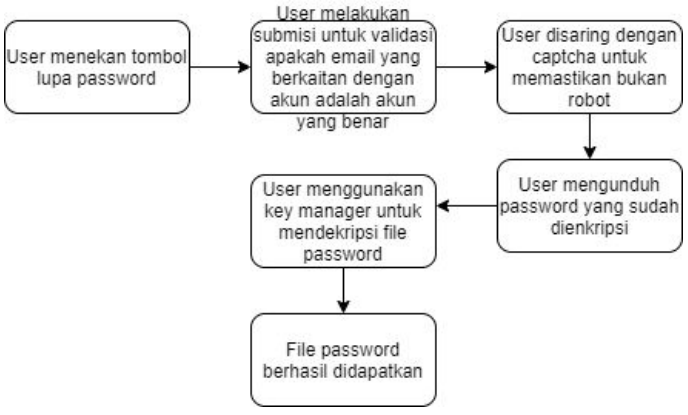
Apabila solusi ini akan diimplementasikan lebih lanjut untuk menjadi salah satu alternatif metode untuk mendapatkan MFA jenis baru maka file private key tersebut dapat digunakan untuk melakukan dekripsi suatu kode yang bersifat hanya bisa digunakan pada waktu itu.

Kode yang bersifat one time password tersebut akan dienkripsi oleh website dengan memanfaatkan public key yang disimpan oleh website saat pertama kali dilakukan pendaftaran oleh pengguna media sosial. Hal ini tidak mengkompromisasikan keamanan karena sifat public key yang tidak dapat digunakan untuk mendeskripsikan data tersebut, jika seseorang memiliki data yang dienkripsi hanya dengan kunci publik tanpa adanya kunci privat maka pada aspek paling praktisnya dia memiliki fungsi hash yang tidak dapat dipecah, kecuali dengan *brute forcing*.

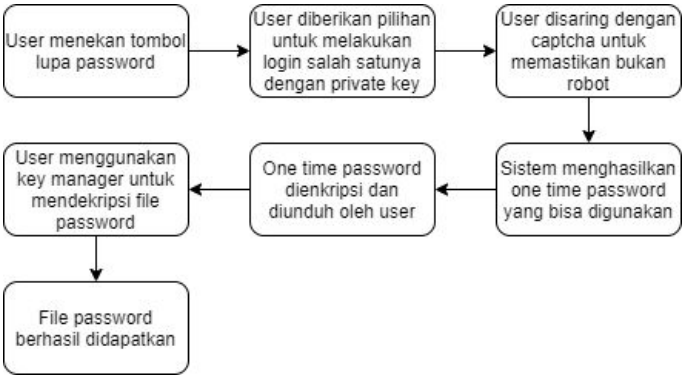
Perlu diperhatikan bahwa skema yang diatas harus diubah sehingga upload private key adalah hal yang wajib:



Lalu langkah untuk melakukan pengingatan password apabila ada pengguna media sosial yang lupa adalah sebagai berikut:



Sedangkan proses untuk melakukan login dengan menambahkan MFA dapat berlaku sebagai berikut:



VII. Analisis

Pendekatan dengan metode ini akan memudahkan proses login yang akan dilakukan user. Karena adanya otentikasi dengan bentuk lain yang tidak mewajibkan pengguna tersebut untuk melakukan hal-hal ekstrem, pada contohnya apabila pada waktu tersebut pengguna harus melakukan reset password dan metode yang tersedia di website harus mewajibkan untuk melakukan reset dan verifikasi ke nomor HP yang sudah tidak digunakan.

Verifikasi dengan private key adalah metode verifikasi baru yang dapat menambah kemungkinan agar pengguna tersebut tidak terkunci secara permanen. Hal ini sering terjadi pada orang-orang Indonesia karena ada kecenderungan untuk berganti-ganti nomor HP untuk mencari nomor HP yang paling baik dan biasanya memiliki bonus kuota internet yang dapat mereka manfaatkan.

Penyimpanan *ciphertext* password dan *public key* para user untuk melakukan enkripsi dalam basis data website tidak akan mengurangi keamanan dari akun yang digunakan karena mereka pada dasarnya teks-teks tersebut akan sulit untuk dipecah dan tidak akan memiliki collision seperti fungsi-fungsi hash. Meskipun begitu perlu juga dipikirkan algoritma mana yang paling tepat digunakan dan paling sesuai dengan use case dari media sosial yang akan digunakan oleh pengguna.

Jika suatu media sosial memiliki kecenderungan untuk digunakan di ponsel atau komputer yang tidak memiliki komputasi tinggi maka akan lebih baik apabila algoritma public key cryptography yang diimplementasikan adalah algoritma ECC atau *Elliptic Curve Cryptography*. Jika pengguna dari suatu media sosial mayoritas adalah pengguna komputer dengan kekuatan yang lebih seperti laptop atau komputer pribadi maka akan lebih kuat apabila digunakan RSA atau ElGamal. Jika sumber daya yang dimiliki berlebih maka akan lebih menarik apabila situs tersebut memberikan pilihan kepada penggunaanya untuk menggunakan skema kriptografi yang seperti apa, sesuai dengan use case yang lebih familiar dan key storage service yang digunakan.

Perlu diingat pula karena komputasi yang dilakukan untuk melakukan enkripsi dan dekripsi public key cryptography adalah komputasi yang berat maka pendekatan dengan melakukan hashing tetaplah perlu dilakukan. Kejadian lupanya password masih harus dianggap sebagai kejadian yang luar biasa dan kegiatan komputasi berat dapat dianggap wajar karena hal tersebut adalah hal luar biasa. Pada saat yang sama apabila pengguna media sosial tersebut menggunakan private key manager seperti Cleopatra maka komputasi dekripsi private key akan dilakukan oleh pengguna sehingga tidak akan

membebani sistem kecuali dalam tahapan enkripsi pada saat user tersebut melakukan pendaftaran.

VIII. Kesimpulan

Keamanan digital di situs web memiliki berbagai rupa, untuk mengamankan informasi pengguna maka dapat digunakan beberapa metode kriptografi. Pada bab-bab sebelumnya telah dibahas bahwa sangatlah mungkin untuk mengimplementasikan kriptografi sebagai bentuk baru dari multi factor authentication, karena private key, yang awalnya hanya diketahui oleh orang-orang yang bergelut di bidang kriptografi akan menjadi suatu wawasan yang diketahui khalayak banyak dan akan digunakan lebih umum. Situs web harus mengakomodir perubahan-perubahan ini

VII. Acknowledgment

Saya berterimakasih kepada bapak Rinaldi Munir karena telah membimbing dalam kelas Kriptografi dan saya berterimakasih kepada Tuhan Yang Maha Esa juga atas mungkinnya terjadi semua ini.

References

[1] What Is the Koobface Virus?. (2020). Retrieved 21 December 2020, from https://www.kaspersky.com/resource-center/definitions/what-is-the-koobface-virus

[2] What is social engineering? Tips to help avoid becoming a victim. (2020). Retrieved 21 December 2020, from https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

[3] Demographics of Social Media Users and Adoption in the United States. (2020). Retrieved 21 December 2020, from https://www.pewresearch.org/internet/fact-sheet/social-media/

[4] Munir, Rinaldi. "Kriptografi Kunci-Publik." IF4020 Kriptografi. 23 Oktober 2020, Institut Teknologi Bandung. Kuliah Tatap Muka

[5] Kioon, Mary & Wang, ZhaoShun & Das, Shubra. (2013). Security Analysis of MD5 Algorithm in Password Storage. Applied Mechanics and Materials. 347-350. 10.2991/isccca.2013.177.

[6] Al-Janabi, Samaher & AlShourbaji, Ibrahim. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management. 15. 1650007. 10.1142/S0219649216500076.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Desember 2020

Muhammad Al Terra 13517145