TUGAS KEAMANAN INFORMASI

Tugas UAS

Di susun oleh:

Muhammad Bagus Nurkahfi

1310651163

Kelas :

D

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

Tugas 1

Kriptografi adalah cara merahasiakan Tulisan yang digunakan sebagai cara berkomunikasi yang aman yang hanya dapat dipahami oleh penerima yang dimaksud saja. Mungkin ketika data sedang dikirim diketahui oleh orang lain, isi data yang harus tetap tidak diketahui kepada pihak ketiga. Data yang dikirim melalui jaringan dan saat tersimpan pada perangkat seperti disk dapat dienkripsi.

Konsep kriptografi dasar diwujudkan oleh semua enkripsi yang kuat dan harus dipahami sebelum belajar tentang implementasi spesifik. Istilah kunci Kriptologi adalah ilmu komunikasi yang aman. Kriptografi menciptakan pesan makna yang tersembunyi; pembacaan sandi adalah ilmu membobol terenkripsi-pesan bijak (pulih maknanya). Banyak menggunakan kriptografi jangka di tempat kriptografi tology, penting untuk diingat kriptologi yang meliputi baik kriptografi dan pembacaan sandi. SEBUAH sandi adalah algoritma kriptografi. SEBUAH plaintext adalah pesan terenkripsi. Enkripsi mengkonversi plaintext ke ciphertext.

Dalam menjaga kerahasiaan data, *kriptografi* mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Dalam arti lain, cryptography adalah seni dan ilmu dalam mengamankan pesan. Dalam dunia kriptografi, pesan disebut plaintext atau cleartext. Proses untuk menyamarkan pesan dengan cara sedemikian rupa untuk menyembunyikan isi aslinya disebut enkripsi. Pesan yang telah dienkripsi disebut ciphertext. Proses pengembalian sebuah ciphertext ke plaintext disebut dekripsi.

Cryptographer adalah orang yang mempraktekkan ilmu kriptografi, sedangkan cryptoanalysts adalah orang yang mempraktekkan kriptanalisis, seni dan ilmu dalam memecahkan ciphertext. Aturan fundamental kriptografi yaitu seseorang harus mengasumsikan bahwa seorang kriptoanalis menguasai algoritma umum enkripsi yang digunakan.

Dengan kata lain, kriptanalis mengetahui cara kerja algoritma enkripsi. Jumlah usaha yang diperlukan untuk menemukan, menguji, dan memasang algoritma baru yang selalu berkompromi atau berfikir untuk berkompromi dengan algoritma lama, akan menyebabkan algoritma baru itu menjadi tidak berguna untuk menjaga kerahasiaan. Sistem kriptografi atau Algoritma Kriptografi adalah sebuah algoritma kriptografi ditambah semua kemungkinan plaintext,ciphertext dan kunci. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Teknik Dasar Kriptografi Terbagi 5 Jenis, yaitu :

1. SUBSTITUSI

Dalam kriptografi, sandi substitusi adalah jenis metode enkripsi dimana setiap satuan pada teks terang digantikan oleh teks tersandi dengan sistem yang teratur. Metode penyandian substitusi telah dipakai dari zaman dulu (kriptografi klasik) hingga kini (kriptografi modern),

Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan *decrypt*. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan *ciphertext* oleh orang yang tidak berhak.

Metode ini dilakukan dengan mengganti setiap huruf dari teks asli dengan huruf lain sebagai huruf sandi yang telah didefinisikan sebelumnya oleh algoritma kunci.

Contoh:

Metode Penyandian Substitusi Sederhana

- **Caesar Cipher**

```
Caesar Cipher
--------------
PLAINTEXT     : BELAJAR BERSAMA
Alphabet      : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Deret Inversi : T E D A B C Z Y X W V U F S R Q P O N M L K J I H G
Kunci         : A = T
----------------------
Encrypt       : EBUTWTO EBONTFT
Decrypt       : BELAJAR BERSAMA
```

2. BLOCKING

Sistem enkripsi ini terkadang membagi plaintext menjadi beberapa blok yang terdiri dari beberapa karakter, kemudian di enkripsikan secara independen.
Caranya :

Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya.

Contoh :

6	J		M	BLOK 1
	A	B	A	BLOK 2
B	R	E		BLOK 3
E		R		BLOK 4
L		S		BLOK 5
A		A		BLOK 6

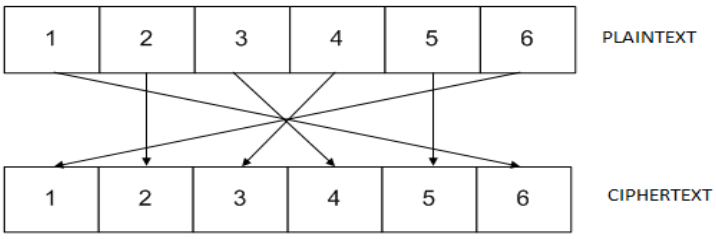
PLAIN TEXT = BELAJAR BERSAMA

ENCRYPT = 6J M BRE E R E R L S A A

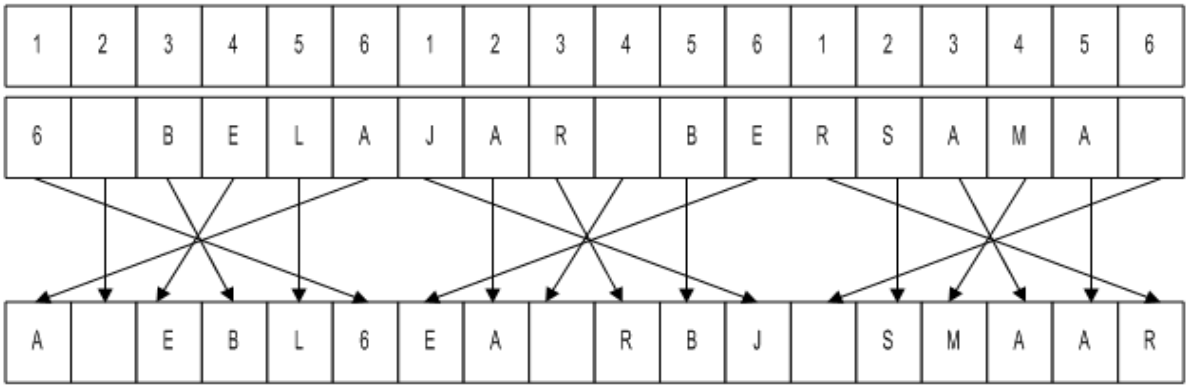
3. PERMUTASI

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.
Caranya
Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.

Plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi, sebagai berikut :



Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :



PLAINTEXT = BELAJAR BERSAMA

CIPHERTEXT = A EBL6EA RBJ SMAAR

4. EKSPANSI

Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran “an”. Jika suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran “i”.

Contoh :

PLAINTEXT : BELAJAR BERSAMA

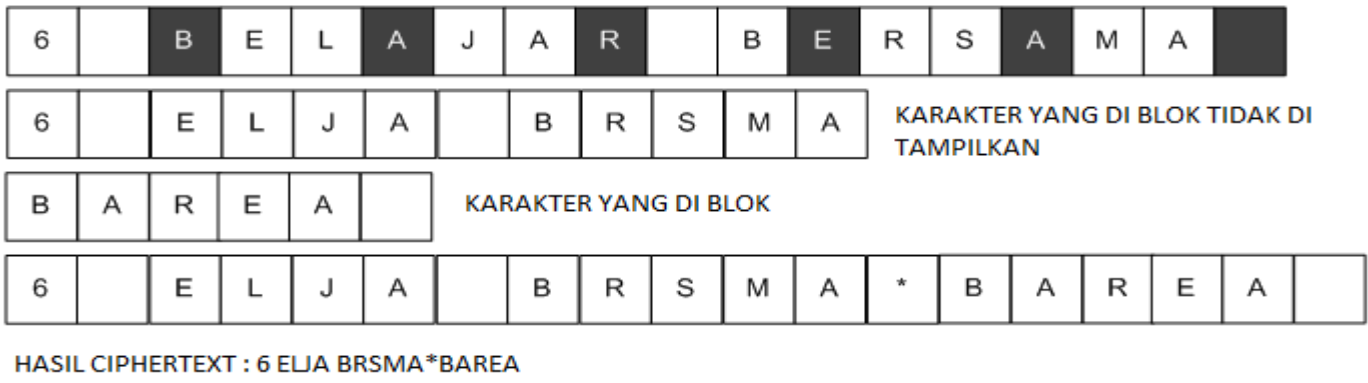
CIPHERTEXT : 6i ELAJARBAN ERSAMABAN

5. PEMAMPATAN

Mengurangi panjang pesan atau jumlah bloknya dengan cara lain untuk menyembunyikan isi pesan.

Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai “lampiran” dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini menggunakan ” * “.

Contoh :



Contoh Kriptografi

Kriptografi Caesar

Salah satu kriptografi yang paling tua dan paling sederhana adalah kriptogtafi Caesar. Menurut sejarah, ini adalah cara Julius Caesar mengirimkan surat cinta kepada kekasihnya Cleopatra. Dalam kriptografi Caesar, maka setiap huruf akan dituliskan dalam huruf lain hasil pergeseran 3 buah huruf. Kriptografi Caesar ini adalah kriptografi substitusi karena setiap huruf akan digantikan huruf lain.

Sebagai contoh, huruf A akan digeser 3 huruf menjadi huruf D, B akan digeser 3 huruf menjadi E, J akan digeser menjadi M, O akan menjadi R dan seterusnya. Pergeseran ini juga berputar kembali ke awal abjad sehingga sesudah huruf Z diikuti kembali oleh huruf A. Kriptografi Caesar ini dikenal sebagai monoalphabetic substitution cipher karena satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain.

Perubahan pada kriptografi Caesar bisa dituliskan sebagai berikut:
Jika Caesar akan menuliskan kalimat ‘I LOVE YOU’ maka akan dituliskan dalam kalimat ‘L ORYH

BRX‘.

Jika kita memberi nomor ke pada huruf-huruf abjad dan kita mulai dengan huruf A=0, B=1, C=2 dstnya

sampai dengan Z=25, maka kriptografi Caesar memenuhi rumus

C = (P + 3)

mod 26,

di mana C adalah nomor abjad ciphertext, P adalah nomor abjad plaintext .

Dan dekripsinya adalah

$P = (C - 3)$

mod 26.

Kriptografi Vigenere

Pada kriptografi Caesar pergeseran akan sama pada seluruh pesan. Jika kunci yang digunakan adalah huruf E, maka setiap huruf pada pesan akan bergeser 4 huruf. Begitu juga bila digunakan kunci-kunci lainnya. Pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda [Sta03]. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext.

Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext. Kriptografi Vigenere ini dikenal sebagai polyalphabetic substitution cipher, karena enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda. Pergeseran setiap huruf pada plaintext ditentukan oleh huruf pada posisi yang sama dan pergeseran ini ditentukan oleh tabel yang sama dengan tabel pada kriptografi Caesar.

Rumus kriptografi Caesar tetap berlaku pada kriptografi Vigenere, baik pada enkripsi maupun dekripsi:

$C=E(P)=(P+k)$

mod26

$P=D(C)=(C-k)$

mod26

di mana P adalah plaintext, C adalah ciphertext, k adalah pergeseran huruf sesuai dengan huruf pada posisi huruf pada plaintext.

Sebagai contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kunci ini akan diulang sama panjang dengan plaintext. Setiap huruf pada kata BESOK mempunyai pergeseran yang berbeda, sehingga setiap huruf akan mengalami pergeseran yang berbeda. Huruf yang sama bisa menghasilkan cipher yang berbeda.

Ada cara lain untuk melakukan kriptografi Vigenere yaitu dengan menuliskan abjad berurutan dari A sampai dengan Z, kemudian kata kuncinya dituliskan secara vertikal di bawah huruf A. Setiap huruf dari kata kunci ini kemudian dilengkapi dengan abjad selanjutnya dalam urutan alfabet dan setelah huruf Z kembali lagi ke huruf A,B dan seterusnya. Untuk melakukan enkripsi terhadap suatu pesan, maka cari posisi setiap huruf pada plaintext pada baris paling atas, kemudian cari huruf pada lokasi yang sama di baris bawahnya. Huruf pertama diubah dengan huruf yang ada pada posisi yang sama pada baris ke dua atau baris dari huruf pertama pada kata kunci.

Huruf ke dua pada plaintext dikonversi dengan huruf pada posisi yang sama pada baris selanjutnya. Huruf ketiga dikonversi dengan baris ke tiga dan seterusnya. Jika semua baris sudah terpakai maka kembali ke baris paling atas dari kata kunci, sampai semua huruf pada plaintext dienkripsi.

Cara lain untuk melakukan kriptografi Vigenere adalah dengan menggunakan tabula recta sebagai berikut : Baris paling atas adalah alfabet dari A sampai dengan Z. Di baris ke dua, tuliskan alfabet mulai dengan B sampai dengan Z kemudian kembali ke A. Di baris bawahnya C diikuti alfabet selanjutnya sampai dengan Z dan kembali lagi ke A. Sampai huruf Z. Cara penulisan ini dikenal sebagai tabula recta. Kemudian enkripsi dilakukan sama dengan enkripsi menggunakan Table 4. Huruf-huruf pada kata kunci sebagai huruf pertama pada baris-baris pada tabula recta dan huruf-huruf pada plaintext dicari di baris pertama tabula recta.

Kriptografi Autokey

Kriptografi Autokey adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kedua kriptografi sebelumnya. Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi.

Rumus yang berlaku untuk kriptografi Autokey sama dengan untuk Caesar dan Vigenere.

$C=E(P)=(P+k)$

mod26

$P=D(C)=(C-k)$

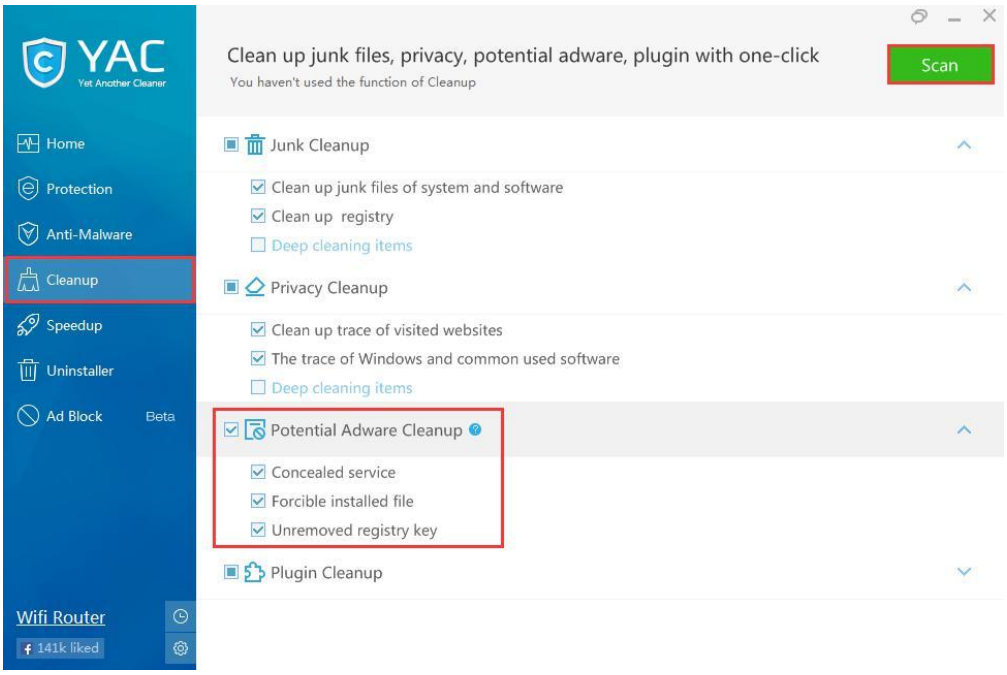
mod26

Contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA. Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere.

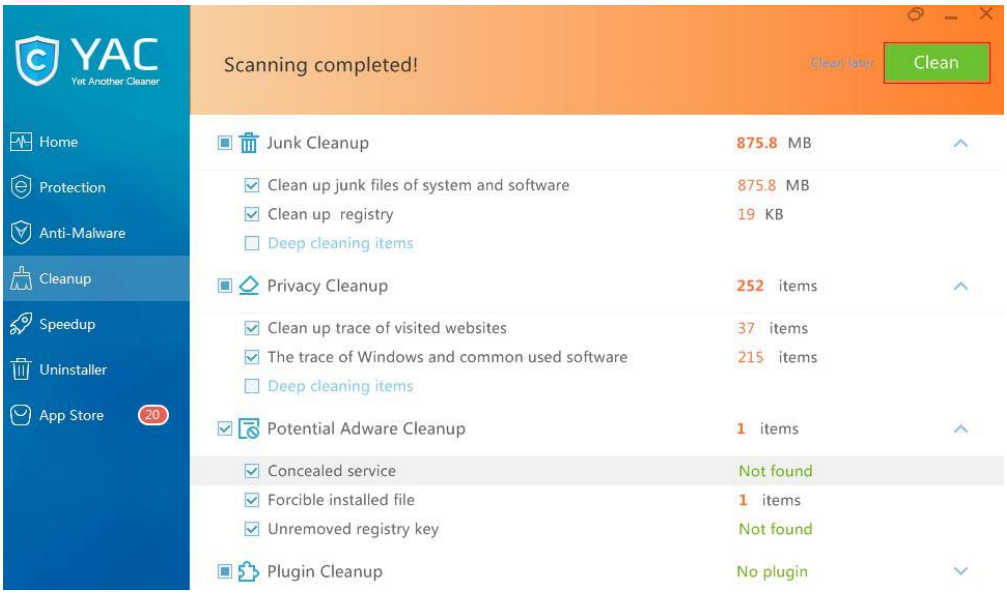
Tugas 2

1. Instal PC Cleaner YAC di PC kita.

2. Setelah terinstal, buka program, beralih ke "Pembersihan" fungsi, dan kemudian klik pada tombol "Scan".



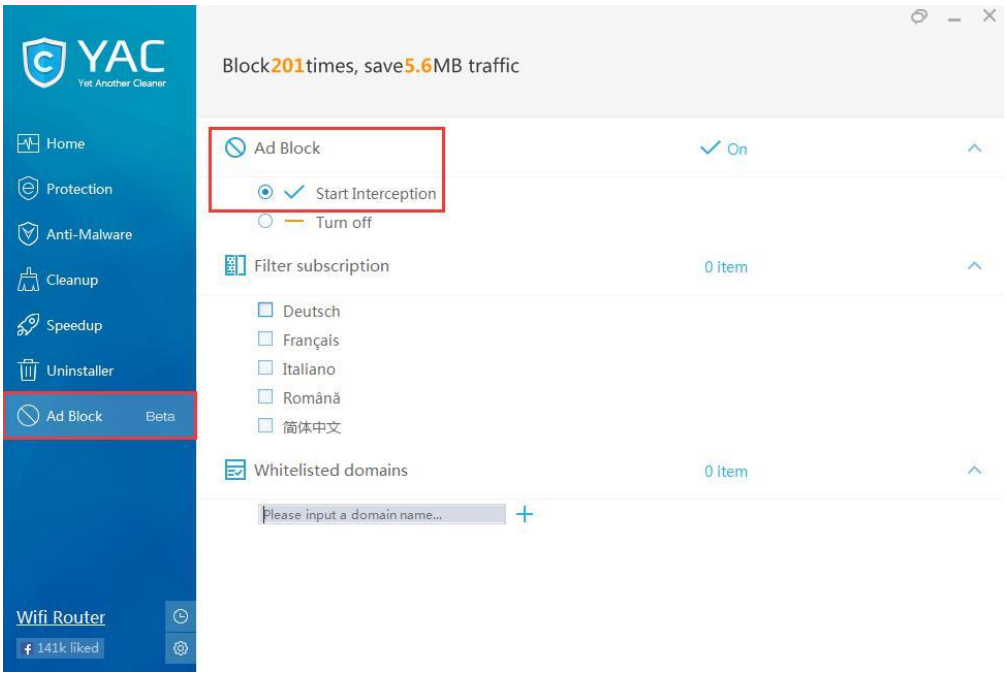
3. Kemudian YAC dapat membantu Kita membersihkan semua adware tersembunyi di PC Kita, dan Kita dapat mengklik "Clean" untuk menyelesaikan semua cleanup.



Tips

Lebih jauh lagi, Kita juga dapat menyingkirkan potensi popup iklan, spanduk dan semua iklan menjengkelkan dengan menggunakan "block Iklan" fungsi, YAC

akan menampilkan bersih dan murni on-line pengalaman berselancar.



CARA MEMINDAHKAN allinone keylogger MANUAL

Untuk menghapus allinone keylogger secara manual Anda harus memiliki pengetahuan teknis pertama maka hanya Anda dapat menghapusnya secara manual karena memerlukan pengetahuan tentang sistem file dan file registry dan jika Anda tidak punya ide tentang hal ini kemudian mencoba metode manual dapat menyebabkan Anda untuk situasi yang lebih bermasalah dan satu penghapusan file yang salah dapat membuat sistem anda benar-benar tidak dapat digunakan.allinone keylogger Langkah-langkah untuk Penghapusan manual adalah:

Hapus allinone keylogger dari Windows XP

- Pilih safe mode dan kemudian tekan tombol enter.
- Jalankan file control.exe.

Hapus allinone keylogger dari Windows 7

- Tekan tombol jendela + r.
- Ketik regedit dan tekan enter.

Hapus allinone keylogger dari Windows 8

- Klik pada tombol start dan pergi ke panel kontrol.
- Klik pada penampilan dan personalisasi.

Hapus allinone keylogger dari Windows Vista

- Restart komputer ke safe mode dengan jaringan.
- Reboot komputer yang terinfeksi.