

# SIMULTAN CONTRACT SIGNING WITHOUT AN ARBITRATOR (USING CRYPTOGRAPHY)

Agung Nursilo

[www.noersilo.web.id](http://www.noersilo.web.id) | [noersilo@yahoo.com](mailto:noersilo@yahoo.com)

Protokol ini menggunakan pendekatan baby step. DES digunakan dalam protokol ini, walaupun banyak algoritma lainnya.

1. Alice dan Bob memilih  $2n$  kunci DES secara acak, dan dipasangkan. Kunci tersebut dikelompokkan dengan cara itu untuk protokol.
2. Alice dan Bob mengenerate  $n$  pasangan pesan,  $L_i$  dan  $R_i$ . Dikiri adalah setengah tanda tangan, dan dikanan adalah setengahnya dari tanda tangan yang dikiri. Koneksi akan masuk jika pihak dapat menghasilkan kedua bagian itu.
3. Alice dan Bob mengenkripsi pasangan pesan pada setiap pasangan kunci DES, pesan kiri dengan kunci kiri dan pesan kanan dengan kunci kanan.
4. Alice dan Bob mengirim masing-masing kumpulan  $2n$  pesan terenkripsi lainnya.
5. Alice dan Bob mengirim masing-masing setiap pasangan kunci menggunakan *oblivious transfer protocol* untuk setiap pasangan. Maka dari itu, Alice mengirim Bob kunci yang digunakan untuk mengenkripsi pesan kiri atau pesan kanan, saling bebas untuk setiap pasangan  $n$ . tidak pada Bob. Mereka dapat mengirimkan alternatif setengah atau dapat mengirim 100 dan tidak ada masalah. Sekarang Alice dan Bob memiliki satu kunci dari setiap pasangan kunci, tetapi tidak ada yang tahu dimana yang satunya lagi.
6. Alice dan Bob mendekripsi sebagian pesan yang mereka bisa menggunakan kunci yang diterima. Mereka meyakini dekripsi pesan adalah valid.
7. Alice dan Bob mengirim setiap bit pertama dari semua  $2n$  kunci DES.
8. Alice dan Bob mengulang langkah ke-7 untuk bit kedua dari semua  $2n$  kunci DES, bit ketiga dan seterusnya sampai semua bit dari kunci DES yang ditransfer.
9. Alice dan Bob mendekripsi sebagian pasangan pesan dan kontraknya di signing.
10. Alice dan Bob menukar kunci privat yang digunakan selama *oblivious transfer protocol* pada langkah ke-5 dan masing-masing memverifikasi bahwa pihak lain tidak mencuri.

Kenapa Alice dan Bob melakukan hal tersebut? Kita asumsikan Alice ingin mencuri dan melihat apa yang terjadi. Pada langkah 4 dan 5, Alice ingin mengganggu protokol dengan mengirim *nonsense bit string* Bob. Bob mengaitkan langkah 6, ketika dia mencoba

mendekripsi sebagian yang dia terima. Bob melakukannya dan berhenti dengan aman, sebelum Alice dapat mendekripsi beberapa pasangan pesan Bob.

Jika Alice sangat pintar, dia akan mengganggu sebagian protokol. Dia dapat mengirim satu bagian setiap pasangan yang tepat, tapi mengirim *string* palsu untuk bagian lainnya. Bob mempunyai 50 persen kesempatan dari sebagian pesan benar yang diterima, jadi sebagiannya lagi dapat Alice curi. Bagaimanapun, hal ini bekerja jika terdapat satu pasang kunci. Jika terdapat 2 pasang kunci, penipuan dapat berhasil sebesar 25 persen. Karena itu  $n$  harus besar. Alice mempunyai perkiraan output tepat dari  $n$  *oblivious transfer protocol*, dia memiliki 1 pada  $2n$  kesempatan yang dilakukan. Jika  $n=10$ , Alice mempunyai 1 pada 1024 kesempatan menipu Bob.

Alice dapat juga mengirim bit acak Bob pada langkah 8, mungkin Bob tidak tahu bahwa dia mengirim bit acaknya hingga menerima seluruh kunci dan mencoba mendekripsi sebagian pesan. Dia siap menerima sebagian kunci, dan Alice tidak tahu sebagiannya. Jika  $n$  cukup besar, Alice yakin mengirim *nonsense* bitnya untuk kunci yang siap diterima dan dia tahu bahwa dia mencoba menipunya.

Mungkin Alice akan melakukan langkah 8 hingga mempunyai cukup bit dari kunci untuk menghindari *brute force attack* dan kemudian menghentikan alur bit. DES memiliki 56 bit panjang kunci. Jika Alice menerima 40 dari 56 bit, dia cukup mencoba 216 atau 65536 kemungkinan kunci. Bob dapat melakukan hal yang sama.

Alice adil, karena dia hanya sedikit mengelabui. Dan diakhir protokol, kedua pihak mempunyai  $n$  pasangan pesan yang disigning, terdapat satu yang *signature*-nya valid.

Salah satu cara Alice dapat mencuri, dia dapat mengirim Bob pesan identik pada langkah 5. Bob tidak dapat mendeteksi hal ini hingga protokol diselesaikan, tetapi Bob dapat menggunakan transkrip dari protokol untuk meyakinkan judge dari duplikat Alice.

Terdapat 2 kelemahan dengan protokol tipe ini. Pertama, akan menjadi masalah jika salah satu dari pihak mempunyai kekuatan komputasi yang signifikan lebih baik dari yang lainnya. Contohnya, Alice dapat me-mount brute force attack lebih cepat dari pada Bob, siapa yang tidak dapat melakukan hal yang sama pada kemungkinan waktu amount, akan tidak menyenangkan.

Kedua, masalah muncul jika salah satu pihak menghentikan protokol lebih cepat. Jika Alice tiba-tiba menghentikan protokol, dengan usaha perhitungan yang sama, tetapi Bob tidak memiliki jalan yang lain. Contoh, Kontrak yang sudah ditetapkan dilakukan setiap minggu dan Alice mengakhiri protokol ketika Bob menghabiskan tahun dari kekuatan perhitungan sebelum dia yakin untuk melakukan, itu adalah masalahnya. Kesulitan sesungguhnya adalah kurangnya deadline jangka pendek dimana proses berakhir dengan salah satu atau tidak sama sekali pihak yang membatasi.

[Referensi : Applied of Cryptography](#)