Протокол одновременного подписания контракта

Содержание

- Подписание контракта при помощи посредника
- Одновременная подпись контракта без посредника(лицом к лицу)
- Одновременная подпись контракта без посредника(без личной встречи)
- Одновременная подпись контракта без посредника(с использованием криптографии)

Введение

А и Б хотят заключить контракт. Устно согласие было достигнуто обоими сторонами, но никто не хочет первым ставить свою подпись. При личной встрече такой проблемы бы не было, но на расстоянии это вызывает затруднения.

Подписание контракта при помощи посредника

Действующие лица: А, Б, Т.

Идея: Вводится третье доверенное лицо Т, которое контролирует процесс с обеих сторон.

1. А подписывает копию контракта и посылает Т.
2. Б подписывает копию контракта и посылает Т.
3. Т отсылает сообщение обоим сторонам, что соучастник поставил свою подпись.
4. А подписывает обе копии контракта и посылает Б.
5. Б подписывает обе копии контракта и одну оставляет у себя, другую отсылает А.
6. А и Б говорят Т, что у каждого есть подписанный экземпляр.
7. Т уничтожает свои две копии с единственной подписью на каждом.

Подписание контракта при помощи посредника

Действующие лица: А, Б, Т.

Идея: Вводится третье доверенное лицо Т, которое контролирует процесс с обеих сторон.

Одновременная подпись контракта без посредника(лицом к лицу)

Действующие лица: А, Б.

Идея: А и Б встречаются и каждый пишет по букве своего «имени», пока они не будет написаны полностью.

1. А пишет очередную букву своей подписи и передаёт контракт Б.
2. Б делает тоже самое и возвращает его А.
3. Процесс продолжается, пока обе стороны взаимно не подпишут контракт.

Одновременная подпись контракта без посредника(лицом к лицу)

Действующие лица: А, Б.

Идея: А и Б встречаются и каждый пишет по букве своего «имени», пока они не будет написаны полностью.

Одновременная подпись контракта без посредника(без личной встречи)

Действующие лица: А, Б, *a*(вероятность А), *b*(вероятность Б).

Идея: А и Б обмениваются сообщениями подписанными типа: «Я согласен, что с вероятностью *p* я связан условиями контракта.»
В таком случае получатель такого сообщения может предъявить его и с вероятностью *p* он будет прав, контракт будет считаться подписанным.

1. А и Б согласовывают дату окончания подписания контракта.
2. А и Б договариваются о различии вероятностей, которым они собираются пользоваться.
3. А посылает Б сообщение подписанное с вероятностью $p = a$.
4. Б посылает А подписанное сообщение с вероятностью $p = a + b$.
5. Пусть *p* - это вероятность из сообщения полученного А от Б на предыдущем шаге. А посылает Б подписанное сообщение с $p' = p + a$ или 1, смотря что меньше.
6. Пусть *p* - это вероятность из сообщения полученного Б от А на предыдущем шаге. Б посылает А подписанное сообщение с $p' = p + b$ или 1, смотря что меньше.
7. А и Б продолжают выполнять (5) и (6), пока оба не получат сообщения с вероятностью $p = 1$ или пока не наступит дата из 1го шага

Одновременная подпись контракта без посредника(без личной встречи)

Действующие лица: А, Б, *a*(вероятность А), *b*(вероятность Б).

Идея: А и Б обмениваются сообщениями подписанными типа: «Я согласен, что с вероятностью *p* я связан условиями контракта.»

В таком случае получатель такого сообщения может предъявить его и с вероятностью *p* он будет прав, контракт будет считаться подписанным.

Одновременная подпись контракта без посредника(с использованием криптографии)

Действующие лица: А, Б.

Идея:

1. А и Б случайно выбирают 2*n* ключей DES, сгруппированных попарно.
2. А и Б создают *n* пар сообщений L_i и R_i, например, «Это левая половина моей *i* - той подписи» и «Это правая половина моей *i* - той подписи», *i* = 1, …, *n*. В каждое сообщение также будет входить цифровая подпись контракта и временная метка. Контракт считается подписанным, если другая сторона может предъявить обе половины L_i и R_i одной пары подписей.
3. Обе стороны шифруют свои пары сообщений парами ключей DES, левое сообщение — левым ключом в паре, правое — правым.
4. А и Б посылают друг другу свои пачки из 2*n* шифрованных сообщений, поясняя, какие сообщения какими половинами каких пар являются.
5. А и Б посылают друг другу все пары ключей используя протокол рассеянной передачи для каждой пары. То есть, А посылает Б независимо для каждой из *n* пар ключей, либо ключ, использованный для шифрования левого сообщения, либо ключ, использованный для шифрования правого сообщения. Б делает также. Они могут посылать свои половинки по очереди, или сначала один может послать все, а потом другой — НЕВАЖНО. Теперь и у А и у Б есть по одному ключу из каждой пары, но никто не знает какие из половинок получил соучастник.

Одновременная подпись контракта без посредника(с использованием криптографии)

Действующие лица: А, Б.

Идея:

Одновременная подпись контракта без посредника(с использованием криптографии)

Действующие лица: А, Б.

Идея: