# Слепая подпись

Подготовила
Валерия Соколова

# Определение

**Слепая подпись** разновидность ЭЦП, особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа.

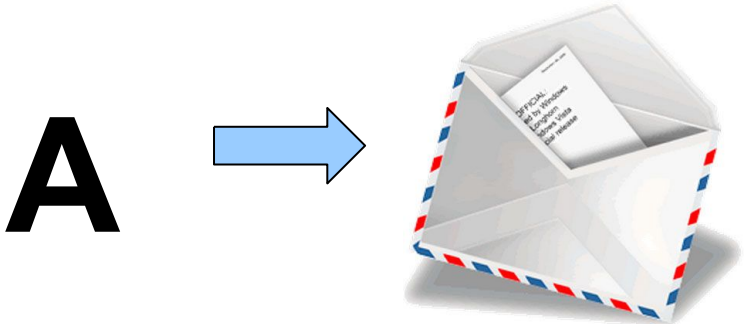
Дэвид Чаум 1982 год

# Основная идея

Отправитель А шифрует документ и посылает его стороне В.


Сторона В, не видя содер[illegible] имени, подписывает его и возвращает обратно стороне А.

Сторона А снима[illegible] ифр, оставляя на документе только [illegible] стороны В.

# Свойства

**Нулевое разглашение**.
**Непрослеживаемость**.
**Неподложность**.

Подписывающую сторону не обманут (никакого использования во вред)

# Полностью слепая подпись

Начальное сообщение

Алиса зашифровывает
и отправляет Бобу


$$c = f(m).$$

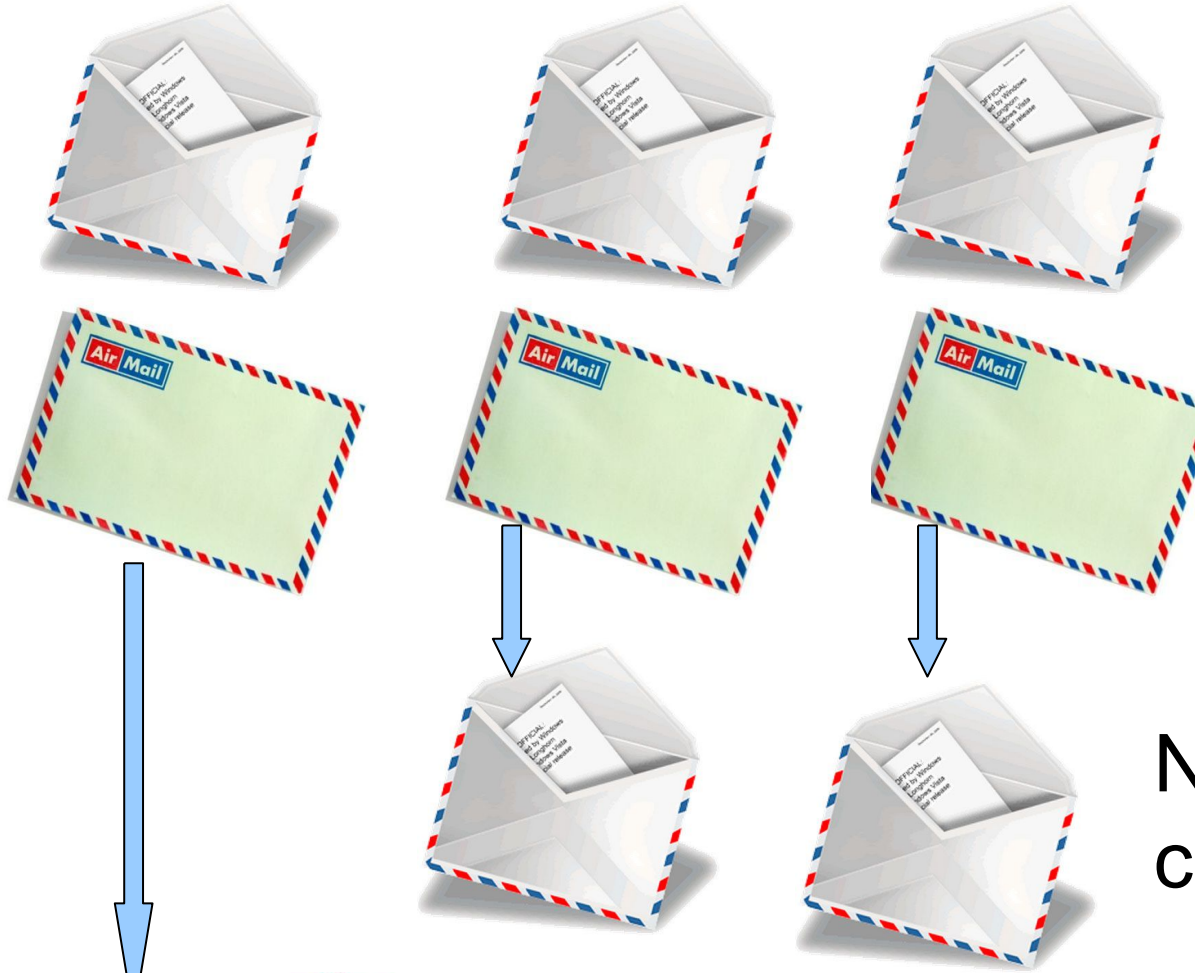
Боб подписывает и отправляет
обратно

Алиса получает
свое шифрован

$$c' = g(c) = g(f(m)).$$

$$c'' = g(f(m)) * f^{-1} = g(m).$$

# Слепая подпись




N сообщений Боба

N зашифрованных сообщений Боба

N-1 расшифрованных сообщений Боба

Подписанное слепой подписью письмо

# Слепая подпись Чаума

Рассмотрим протокол «слепой» подписи Чаума, основанный на криптосистеме RSA. Пусть субъект A желает подписать открытое сообщение M у субъекта B, но при этом абонент A не хочет, чтобы абонент B знал содержание подписываемого им сообщения.

Для выполнения этой процедуры надо осуществить следующие шаги:

1. Абонент A выбирает случайным образом простое число k, которое должно быть взаимно простым с модулем абонента B, по которому выполняются вычисления.
2. Затем он рассчитывает число $M_1 = k^e M \pmod N$, которое и отправляет по открытому каналу связи абоненту B для подписания; *e* – открытый ключ шифрования абонента B. Отметим, что подписывающее лицо не имеет доступа к открытому сообщению M, поскольку оно закрыто «затемняющим» множителем k (в степение) и операцией умножения по модулю.
3. Абонент B подписывает сообщение $M_1$ в соответствии с процедурой подписания документов в криптосистеме RSA: $S = (k^e M)^d = kM^d \pmod N$.
4. Сформировав подпись S, абонент B не имеет доступа к значению $M^d$, поскольку оно зашифровано множителем k. Если бы подписавший смог узнать число $M^d$, то он мог бы легко прочесть открытое сообщение M, так как $(M^d)^e = M \pmod N$.
5. Абонент B отправляет число $M^d$абоненту A. Абоненнт A с помощью расширенного алгоритма Евклида находит для числа k мультипликативно обратный элемент ($k^{-1}$) в кольце вычетов по модулю N и восстанавливает электронную подпись («снимает» затемняющий множитель k): $k^{-1}S = k^{-1}kM^d = M^d \pmod N$.

В результате субъект A получил подпись абонента B на сообщении M, причем у него есть уверенность в том, что абонент B не знает содержания им же подписанного документа.

# Банковская сфера

# Тайное голосование

## ГОСТ Р 34.10-2001

1) Избирателем устанавливается защищенное соединение с валидатором
2) избиратель генерирует избирательный бюллетень
И хеширует бюллетень
3) Избиратель добавляет к хешу бюллетеня маскирующий множитель и отправляет в-ру
4) Валидатор проверяет: Голосовал ли уже избиратель?
Нет — подписывает замаскированный хэш
5) Избиратель извлекает маскирующий множитель и отправляет бюллетень счетчику
6) Счетчик проверяет корректность подписи, идентификатор и прибавляет голос

Спасибо :-)