

Re: protocol for proofing sending a document

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2029.html>

paul_at_atom.sbrk.co.uk

Date: 06/28/05

Date: Tue, 28 Jun 2005 15:33:38 GMT

In article <d9q0pk\$4a8\$05\$1@news.t-online.com>, Anna Kahn wrote:
> Assume we have 2 parties Alice and Bob. Alice wants to send a document
> to Bob. If Alice really sends the document to Bob, then she can prove to
> a third, not involved party, Carol, that indeed she sends the document
> to Bob (so Bob received the document) and there is no way for a
> dishonest Bob to claim that he never received the document from Alice.
> Further, if Alice doesn't send the document to Bob, then there is no way
> for Alice to prove to Carol, that she sends the document.

Alice sends Bob an encrypted document. Bob signs encrypted document and sends back to Alice. Alice publishes decryption key to Bob and Carol.

Paul