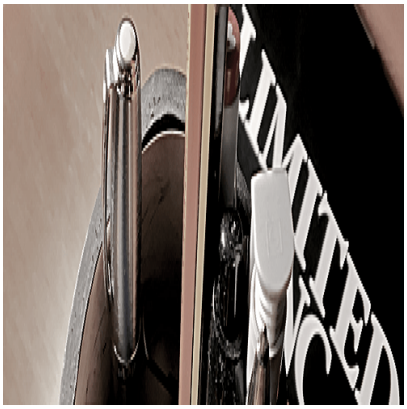


Sign here â?¦â?¦â?¦â?¦â?¦â?¦â?¦â?¦

Description

How do signatures function? A signature is a sign, seal, or mark on a document indicating its authenticity, as when a painter signs a painting, or someone signs a letter or legal document. The signature and the thing it marks is meant to be a one-off. The signature marks an original document, before the thing gets reproduced, copied or repeated.

The philosopher Jacques Derrida made much of the idea of the signature in his book *Limited Inc*. One of his key provocations is that a signature is something that does in fact get repeated. Far from exemplifying an original moment, the signing function depends on the fact that signatories put their signatures on many documents, repeatedly: â??In order to function, that is, to be readable, a signature must have a repeatÂable, iterable, imitable formâ?• (20).

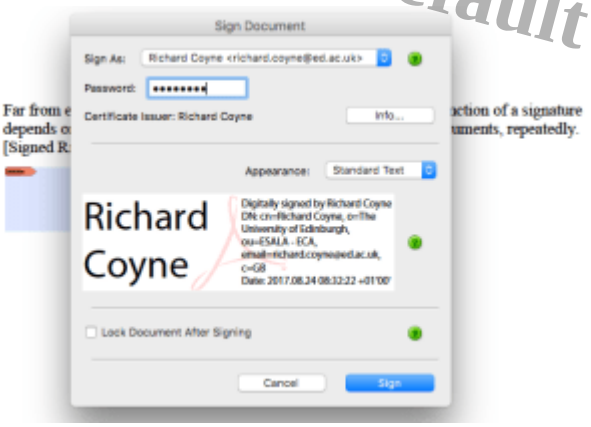
Digital signatures

Digital signatures depend on, multiply, amplify and further problematise the place of repetition in authentication. Iteration and reproduction are key elements in any digital process, not least as creative works get produced, circulated, and protected on line. See post Being David Hockney.

How do digital signatures function? Hereâ??s a worked example. Consider the following short block of text followed by the authorâ??s name, time and date. This could be a text or email message, or a line in a contract that I want to sign off. It could be just a few lines or a whole book.

> Far from exemplifying an original, one-off, singular moment, the function of a signature depends on the fact that signatories put their signatures on many documents, repeatedly. [Signed Richard Coyne 8:26 am 24 August 2017]

Just including text that states Iâ??ve signed it is not enough. I can also sign this content digitally by placing it in a word processor document and adding in a scanned picture of my signature. But that doesnâ??t prevent the document from being changed or faked. PDF editors such as Adobe Acrobat provide a more formal and trusted signing mechanism. I can sign the document in Adobe Acrobat and secure the signature with a password.



Behind the scenes of a digital signature system

How does such a digital signature work? To demonstrate to myself how digital signing works, I have replicated the process in a Google Spreadsheet, with program scripts that provide functions to encrypt a string of text, and also generate a hash. (See posts Decode this and Immutable data.)

So I can call up a function to generate a hash of the document content. I used the MD2 hash algorithm to generate a standard 32 character long unique (almost) encoding of the document content above:

> 775ce28d00898cf8334881ea5fb43381

The hash is used as a method of authentication. If even just one character in the original message is changed then the hash will look different. E.g. if someone adds a full stop at the end of the paragraph then the hash will be

> acbcfdbf4e3479b884ae256fbfa84757

The MD2 hash algorithm (along with other hash standards) is well known, and coded into various digital signature systems. There is no way of reverse engineering a hash into the original text it was derived from. The function of the hash is to indicate whether or not a block of text has been altered.

Encrypting the hash

Perhaps the hash could serve as a signature, or at least authentication of the original document. The hash could be attached to the document to form part of a test that the document has not been tampered with. But anyone could create a document and its MD2 hash and claim to be the signatory. This is where encryption comes in.

The signature software encrypts the hash. Text is encrypted with an encryption key. Encryption turns a block of text into something that is unreadable unless you have the key to decrypt it: the decription key. In the case of a digital signature system there needs to be both a private and a public key. The software used by the signatory encrypts the hash with the secret private key (or password), and anyone else can decrypt this with the publicly available *public* key.

Someone who wants to check the authenticity of the signed document when I email it to them uses the public key. So they need to be notified of this public key, and that it belongs to my signature. (I think the public key is a bit like a royal seal that monarchs used to cast in wax to indicate that the document has come from the monarch. Everyone knows the seal, i.e. the crest, insignia, of the monarch. Itâ??s no a secret.)

I used an arbitrary encryption key 0CB50746C4008BD9, and a public decryption key â??LimitEdâ?• to turn the hash (not the original document) into

8C16D5BA0010627AD9E200DB07BA2D9FCBDC14CAD466EDCF36D011CE96398C31

That string of arbitrary looking characters gets stored with the original document, and constitutes its signature. The signature is an ***encrypted hash of the original document***.

The recipient of the document (i.e. the receiving software) then checks its authenticity by decrypting the long string signature using the public decryption key (â??LimitEdâ?•). That recreaters the hash of the original document: acbcfdbf4e3479b884ae256fbfa84757.

The receiving software then uses the MD2 hash algorithm to generate a hash of the received document. If that is different to the decrypted hash then the document has been tampered with.

Like a signed letter, the original document can be copied and transmitted any number of times, and anyone can read its content. The content of the message is not encrypted; just the hash.

Arun Sundararajan puts this method succinctly in a chapter on blockchain technology: â??This allows for a simple way to create a â??signatureâ??: since you are the only person who has your private key, then a message encrypted with it could only have come from you. And since your public key is public, anyone can verify that this is your signatureâ?• (88).

Being able to authenticate documents with a signature is important in the case of â??smart contracts,â?• shared contracts that are built on peer-to-peer blockchain technology.

Chains of encryption

I couldnâ??t work out how to implement a function that has an encryption key (private) that is different to a decryption key (public). So I encrypted the public key using a 3rd master encryption key. So the private key is an encrypted version of the public key. Confused? If nothing else this process highlights how pervasive are the chains of encrypted encryptions, encrypted hashes, and hashed encryptions in the digital economy.

References

- Derrida, Jacques. 1988. *Limited Inc*. Trans. Samuel Weber. Evanston, IL: Northwestern University Press
- Shadowman. 2017. How does a public key verify a signature? *Stackoverflow*, 15 August. Available online: https://stackoverflow.com/questions/18257185/how-does-a-public-key-verify-a-signature (accessed 24 August 2017).
- Sundararajan, Arun. 2016. *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*. Cambridge, MA: MIT Press

Note

- Hereâ??s a more complete quote from Derrida: â??Effects of signature are the most common thing in the world. But the condition of possibility of those effects is simultaneously, once again, the condition of their impossibility, of the impossibility of their rigorous purity. In order to function, that is, to be readable, a signature must have a repeatÂable, iterable, imitable form; it must be able to be detached from the present and singular intention of its production. It is its sameness which, by corrupting its identity and its singularity, divides its seal [*sceau*]â?• (20). The French word for seal is *sceau*, a term that Derrida plays about with in other parts of his essay, particularly in relation to name of his adversary in this essay, the language philosopher John Searle.

Category

1. Economics

Tags

1. blockchain
2. ciphercity
3. cryptography
4. economics
5. hash

Date Created
August 26, 2017
Author
rcoyne99