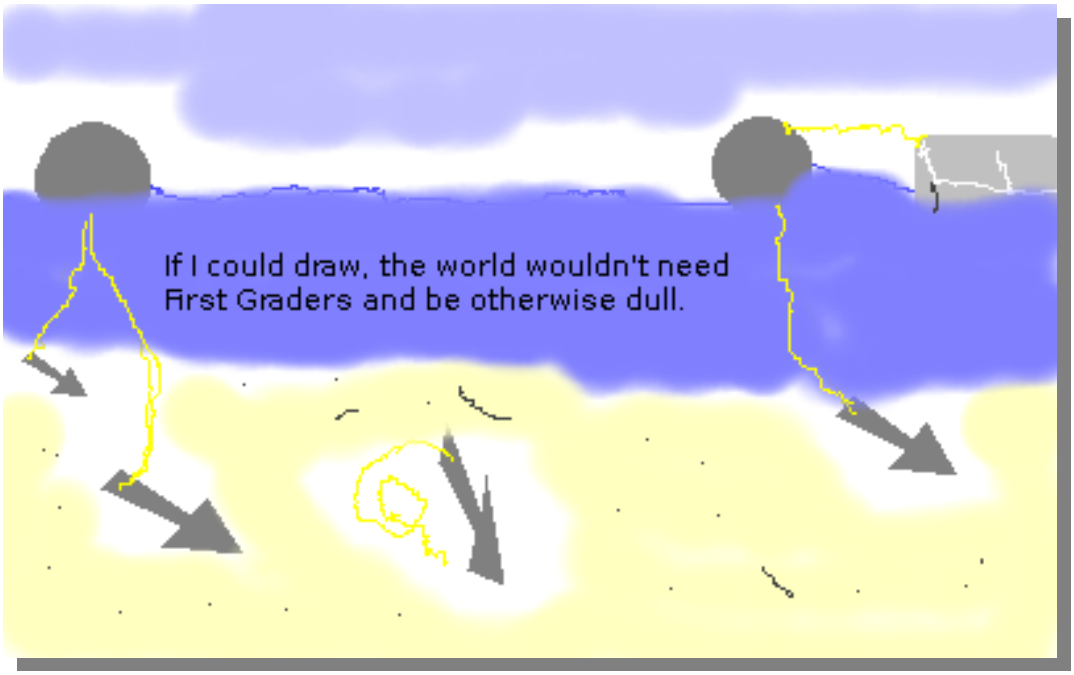
**Connecting the dots**

***A simple visualization of RUST Technology.***



# Introduction

There are well known and accepted design principles for cryptographic systems (see Methods). While Redact Unless Static Text (RUST) Technology may seem at first the antithesis, "Security through Obscurity", there are facets of meta data transmission similar to a traditional cipher.

Oddly, the design principles for a cipher make no mention of a "round-trip". That is, that the design principals can be interpreted as to apply only to the entity issuing (enciphering) a message and need not apply to the same degree to an entity receiving (and presumably deciphering) the message. Imagine for a moment that this is not an oversight, and that there are embedded parts of some messages like *Personally Identifiable Information*, never meant to be deciphered, except as properties, attributes or specific associations well known by the message issuer and message recipient.

So, the question: *Is RUST a cipher?*

## Methods

We introduce Anchor●Buoy●Boat Diagrams.

Rules:

I. Chains start with an Anchor

II. followed by any number of [●Buoy●Boat]

III. and end with [●Buoy●Anchor]

IV. so in this fashion the chains always begin and end with an Anchor.

V. Investigations (deciphering, connecting the dots etc.) proceeding from left to right are impeded due to ambiguity (≥Ambiguity≥)

VI. and from right to left are constrained by anonymity (≤Anonymity≤).

A [●Buoy●Anchor] or a [●Buoy●Boat] is a piece of information paired with it's (PII) class name – a document with RUST Technology applied would, by default, substitute one for the other in printed or other copies.

Cryptography Design

1. The system must be practically, if not mathematically, indecipherable;
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;
5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

   -- Kerckhoffs' principle

## Results

The null chain is Anchor•Buoy•Anchor and corresponds to self awareness.

*John Doe's nickname is "Binky".*

Anchor•Buoy•Anchor
John Doe•[aka]•"Binky"

decryption: John Doe is called "Binky".

The need for corroboration is obvious to any reasonable investigator, but the subtle change in the diagram result may not be so clear.

*John Doe's friend Dr. Bill Jones calls John "Binky".*

Anchor•Buoy•Boat•Buoy•Anchor
John Doe•[bystander]•Dr. Bill Jones•[contact]•Binky
John Doe•[bystander]•[contact]•Binky

decryption: John Doe's friends call him "Binky".

Let's try something a little more complicated, and useful.

*John Doe's wife, Jane (Jones) Doe, has a brother, Dr. Bill Jones, who is a member of the AMA.*

Anchor•Buoy•Boat•Buoy•Boat•Buoy•Anchor
John Doe•[bystander]•Jane (Jones) Doe•[dna]•Dr. Bill Jones•[groups]•American Medical Association
John Doe•[bystander]•[dna]•[groups]•American Medical Association

decryption: John Doe knows somebody with a relative who belongs to the AMA.

| Kerckhoffs | RUST |
|---|---|
| The system must be practically, if not mathematically, indecipherable; | Once redacted, information is practically irretrievable. Forensic examination techniques of storage media with "memory" have come a long way since 1883. Still, once redacted *and moved to fresh media*, the information becomes mathematically indecipherable. |
| It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience; | Copies of the document do not enlighten any recipient as to the original private content. Sub-categories are public. Public Categories of PII |
| Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents; | The "key" in this case is distributed switches affecting the content of the document copy. However there is nothing here which precludes common knowledge or shared experience – in short *culture*. |
| It must be applicable to telegraphic correspondence; | Based upon the problems William Thompson (Lord Kelvin) encountered building the trans-Atlantic cable at about the same time, we should read this somewhat differently. As in the first principle media must not have "memory", a code must be amenable to simultaneous transmission, although we now know there is no such thing, the fastest transmission pipe extant. |
| It must be portable, and its usage and function must not require the concourse of several people; | Not a fan of military "out-sourcing", we gather. Nonetheless the "concourse of several people" *does preclude culture*. |
| Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe. | As FedEx put it, "So easy even the Chairman-Of-The-Board can do it.". The key to successful security is the motivation and the means to mind your own business. |

## Discussion

1. The null case corresponds to self-awareness and from an investigator's point of view, self-incrimination. It is a simple confession. Veracity is indeterminate.

2. Corroboration in any form should change the resulting diagram to distinguish itself from a parallel confession. As opposed to corroboration, any parallel confession would remain a "lucky guess" no matter how severe the consequences of an unlucky guess. This argues against the utility of data acquisition based on the infliction of high stress; torture. Further (indeterminate) self-incrimination may simply reinforce a case for Mental Illness, rather than provide corroboration of a "fact" originally attested.

3. Both versions of the relation of John Doe to the AMA are true, with or without intermediate detail (specific PII). The intermediate details need not be tested by unreasonable and intrusive means. No detail will make the relationship between the anchors "more true". Since there is no change in outcome, such tests are futile.

4. If any of the "buoys" is deleted then the result is a less refined (and possibly false) description of the relationship. For example:
   John Doe•[groups]•American Medical Association
   decryption: John Doe is a member of the AMA.[1]

   John Doe•[dna]•[groups]•American Medical Association
   decryption: John Doe has a relative in the AMA.[2]

   John Doe•[bystander]•[groups]•American Medical Association
   decryption: John Doe knows an AMA member.[3]

5. If a terminal [Anchor•Buoy•] or [•Buoy•Anchor] is deleted the result is always true, but with less information content. For example:
   John Doe•[bystander]•[dna]•Dr. Bill Jones
   decryption: John Doe knows somebody who is related to Dr. Bill Jones.[4]

   Jane (Jones) Doe•[dna]•[groups]•American Medical Association
   decryption: Jane Doe is related to a member of the AMA.[5]

---

1 This is false.
2 This is close, but not strictly correct.
3 This is true, but less specific and less refined.
4 This is true, with lower specificity.
5 Also true, with lower specificity.

## Conclusions

Without a reference to a "round trip", an exact translation, it is apparent that RUST Technology does convey relationship meta data in both forward (encryption) and backward (decryption) directions and is not incompatible with other design characteristics of a cipher, save one. That is, "It must be portable, and its usage and function must not require the concourse of several people;". Five out of six is not too bad, provided that RUST was designed as a military cipher, but common knowledge and shared experience provides an adequate substitute in the absence of design.

RUST Technology is a type of cipher, when used to introduce ambiguity in the relation truth being transmitted and the diagrams produced show this with directionality characteristics. Turning the diagram around, deciphering against anonymity renders the translation a non-differentiable, but true, instance – not a theory but an opinion. We cannot say though that a RUST cipher can be successfully deciphered in all cases. A puzzle or a cipher of this type need not have any solution (backward) at all or may have many possible, reasonable solutions. One might call RUST, and by reference "Security through Obscurity", a *cultural* cipher rather than a *mathematical* cipher.

In particular, the Anchor●Buoy●Boat diagrams demonstrate that chains of compound probability based on "Security through Obscurity" have an atomic limit in each link – a link cannot be made "more true" - however much that innovation may cost, and is doomed in the sense that making the strongest link stronger does not make a chain stronger. But the bad news unfortunately does not end there because it also implies that there is no possible "back door", always desired by the cryptologist, remembering that we operate only on the strongest link. If cracking the code depends on chains of compounded probability the a "back door" must work starting with the lowest atomic probability.

Although the "Placebo Effect" is real, no drug trial result benefits from more than one placebo – and lowering obscurity by adding the innocent to a list containing the guilty is the same thing – although often accomplished at great cost in currency and civil liberties.

Last, there is some evidence that *cultural* or *natural* ciphers are in use, perhaps bearing the same relationship to military ciphers that "asymmetrical warfare" bears to the more familiar kind. It is known, for example, that terrorists often strike at the same target twice, or more. The World Trade Center was struck twice. Imagine for a moment the operational orders in a cultural cipher.

First Time : Bomb the WTC
Second Time: Fly into a *target of opportunity*.

It can be argued that "Sucking Up to the Boss" or for that matter a "declared strategical genius in residence", who happens to be the Boss's Nephew, can explain the choice of the World Trade Center the second time just as well as an explicit order to that effect. Perhaps it was just a matter of organizational status seeking the second time. As odd as that behavior would seem in a suicide attack; cultural ciphers do not have military discipline.

And, as dangerous as they may be to those whose well-being depends upon cracking the code, the cost in treasure of wringing out obscurity may far exceed the price paid in civil liberty.