TECHNOLOGY SECURITY CONSULTING

A Plausible Pre-History of Cryptography

It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously -- as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. [6]

- David Kahn
The Codebreakers, 1967

Introduction. *Cryptography* is a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use. [5]

The known history of cryptography is well documented. Forty years ago there was published a popular history of cryptography written by David Kahn; today there are several works of this sort. Kahn's book "The Codebreakers" was based on Kahn's earlier work and was written at a time (1967) when the subject of cryptography was 'protected' by National Governments and was not normally discussed outside of that realm[1]. Mr. Kahn's work was updated in 1996 with newer information including sections on the use of cryptography on the Internet [6]. Additionally, during this period (1967 to the present), "new" techniques for "secret communication" have become commonplace as the needs for privacy, security, integrity, and authenticity have become better understood and have become major business challenges.

The U.S. National Security Agency (NSA) has established a museum for cryptography which can be viewed at the National Cryptologic Museum at http://www.nsa.gov/museum/. A virtual or actual tour through the Museum is well worth the time spent.

The many diverse histories of cryptography available to the public present cryptography as if it arose fully established with little precursor activity (see lead quote).

We looked at this question from the point of view of cryptographic primitives[2]. Cryptographic primitives are a necessary, though not sufficient, condition of knowledge to enable cryptography.

We will show that several cryptographic primitives were discovered and used early in human pre-history; we also present an interpretation of how they arose. Since we are dealing in prehistory, those interpretations are certainly not secure.

Cryptography evolved through stages as cryptographic primitives were discovered and used. The pre-historical and historical records of a

[1] In fact, there is some evidence that the National Security Agency was concerned about David Kahn's early publications.

[2] Cryptographic primitives are well-established, low-level cryptographic entities that are frequently used to build cryptographic systems. Primitives are building blocks.

number of civilizations demonstrate the precursors of cryptography from which HTA has formed an evolutionary hypothesis presented herein.

Painting on Stone. We begin with cave paintings that appear around 35,000 BC. These paintings would seem to be the beginning of written communication. [10]

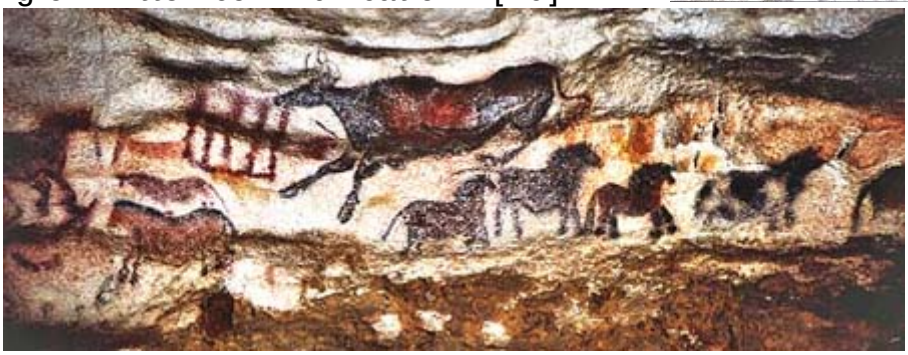

Figure 1 – Representative Cave Drawing.

The first known cave painting as well as the earliest writing was in the form of naturalistic paintings of animals and people drawn in protected places like caves. The pictures of animals were, we think, attempts at honoring and appealing the spirits of the animals that the group needed to kill in the hunt. [9, 10]

Figure 2 - People Perform Actions.

The pictures of people are often done in series, with a figure appearing in several physical positions, representing the positions of a ceremonial dance, or a hunt, or other important function. Gradually over time, primitive cultures stylized their representational messages. [4, 8, 9, 10]

Egyptian Tomb Walls and Monuments. In the Egyptian old kingdom, Dynasty V, texts first occurred in the antechamber of the Pharaoh Unas (aka Unis or Wenis) around 2350 BC.

Of interest to this work are the portions of the inscription, constituting the "book of the dead" in the antechamber of Unas' tomb which must be read in reverse; that is the order of the columns of information is reversed. Additionally, the figures of animals and persons face the "wrong" direction. Archeologists call this "retrograde

Figure 3 - Retrograde Writing from the Tomb of Unas.

writing." [1, 4, 10]

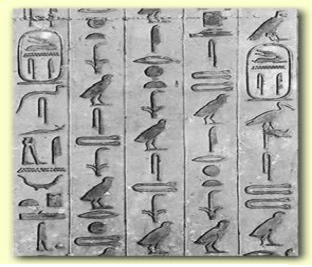

Figure 4- Old Egyptian from the Tomb of Unas.

The actual writing is so-called 'Old Egyptian' which has a great deal of natural redundancy[3]. Interestingly, many of the symbols were also incompletely rendered[4]. The texts are "spells" that the Pharaoh is expected to know in his transition to the afterlife. We do not know why this retrograde writing was used, but it was clearly intentional. It may well be that the direction of the writing and facing of the symbols helped to ensure that the Pharaoh would face the symbols and that his or her reading of the inscriptions would lead in the proper direction to the afterlife[5]. If this is the case then this careful planning shows attention to composition of functions.

Additionally, the Pharaoh would need to provide correct responses to challenges that are given during the passage through the "underworld." Ordering and correct rendering of the spells and texts was very important[6]. These concerns for proper ordering and for reliability are ideas of information integrity and of authenticity. [1]

One might note that the text symbols are highly stylized and precise indicating that much thought has been put into them. In fact, earlier tombs such as the great pyramids of the Giza plateau do not have wall inscriptions, but there are solid arguments that the pyramids themselves were configured to provide the needed information. [4]

It is interesting that from the time of the cave drawings to the time of the first tomb drawings constitutes about 25,000 years during which stylization, in-depth research, and proliferation across cultures developed. [4, 8]

Ancient Cryptography. The inscriptions in the Tomb of Unas are not considered cryptographic, though one could certainly argue that they exhibit transposition (permutation), functional composition, ordered sequence, substitution, and methods to ensure reliability (authenticity

[3] Redundancy is an artifact of ancient language. For example in the Torah or the Bible you will find that phrases are repeated, perhaps in different terms, for emphasis. Redundancy was used to insure that the message was reliably communicated – that is, that its authenticity and integrity were enhanced.
[4] Apparently, there was a fear that the "images" might come to life and threaten the incumbent of the tomb.
[5] Interestingly, though Unas' tomb was the first to use writing to direct the "soul" of the Pharaoh toward "heaven" the earlier pyramid of Khufu has indications of the same technique in its construction.
[6] This is a concern for integrity of message and integrity of the order of messages.

and integrity). It is not believed that retrograde writing was used to "hide" information that was written but was rather used to coordinate the flow of information for the 'deceased' through the underworld. So, let us look at an ancient historical example that is intentionally cryptographic. [1]

The First Acknowledged Cryptography - Substitution. According to Kahn, circa 1900 BC, the tomb of the Egyptian nobleman Khnumhotep II was completed[7]. In one particular section of the inscription, written in hieroglyphics, a master scribe replaced the usual hieroglyphic symbols with new, seemingly nonsensical ones. This act rendered important passages of Khnumhotep's inscription unintelligible except to those who knew what substitution the scribe had made. This is an example of encoding in which an "idea" is substituted for another "idea," and the use of a key needed for interpretation. We do not really know why the substitution was performed, but one can surmise that it was a protective mechanism. Since the text is religious we might also assume that the protection was for religious purposes - that is, to keep sacred knowledge out of the hands of unworthy persons such as tomb robbers. [3, 6, 9, 10]

Figure 5 - Substituted Hieroglyphs from the Tomb of Khnumhoten.

We can see that these substitutions are highly stylized, well planned, and display a great deal of knowledge that we believe must have developed over the centuries, and we have some glimpse of the idea of transposition and of substitution from the Unas sarcophagus some 500 years earlier. The primitives of cryptography, we believe must be found much earlier than 1900 BC and even much earlier than 2400 BC. [6, 8]

Mesopotamian and Egyptian Beer Rationing. In fact, we know that the idea of a functional procedure was well developed early in prehistory. For example the famous Code of Hammurabi, one of civilization's earliest lists of laws (1760 B.C.), includes four paragraphs of regulations that divide beer into 20 different categories. Beer is then rationed according to a formula that accounts both for the category of beer and the status of the recipient;

Figure 6 - Beer Rationing Function.

[7] Some literature imagines that Khumhoten II was a pharaoh, but the Archeological evidence does not support that claim.

that is, functions in at least two independent variables were used. Beer rationing was practiced by both the Mesopotamians and the Egyptians [2, 10].

Egyptian Prehistory. Prior to 30,000 BC, the evidence shows great consistency of cultural adaptations across Africa, Europe, and Asia. Stone tools of similar sorts, both Paleolithic and Neolithic (that is, rough and polished) are abundant.

During this period northern Africa was a very wet environment due to the Mousterian Pluvial - a period of heavy rain that lasted for thousands of years. The Sahara Desert that we know today did not exist, but was a lush vegetative environment with an abundance of animal life. As the Pluvial ended, the landscape began to change to desert. It was at this time that we can see movement of people toward rivers and into communities. The pluvial gave the people of Africa an advantage over European and Asian contemporaries who were faced with ice sheets and very cold weather. Unlike their European "contemporaries" the early Egyptians were still able to engage in hunting large game animals, and since many of the animal herds were now concentrated near the Nile, more stable settlements could be established.

People migrated closer to the Nile as a source of a most precious resource - water. We know of several communities that were established and it is likely during this time that communities began to interact, providing a much wider gene pool on which to draw. We name these communities based upon their “tool industry” rather than from knowledge of language or writing.

The Halfan Industry flourished between 18,000 and 15,000 BC on a diet of large herd animals and fish. Although there are only a few Halfan sites and they are small in size, there is a great concentration of artifacts, indicating that this was not a people bound to seasonal wandering, but one that had settled, at least for a time.

The Fakhurian industry between 17,000 and 15,000 BC was based entirely on microlithic tools. Grinding stones and blades have been found in great numbers with a glossy film of silica on them, possibly the result of grass cutting.

Sebilian (13,000 BC) tools are manufactured from diorite, a hard, black, igneous rock that was plentiful in the area. Sebilian artifacts appear technologically conservative and backward when compared with some of the Upper Paleolithic industries in Europe.

A coexisting industry, called Silsillian (13,000 BC), was a highly-developed microblade industry that included truncated blades, blades of unusual shapes made specifically for one task, and most significant of all, a wide variety of bladelets for mounting onto spears, darts, and arrows. The Silsillian Industry also produced microliths. Microliths are small, fine blades used in advanced tools such as arrows, and harpoons. Also, these blades were used as agricultural tools such as sickles showing that basic farming had begun.

During this time the first great experiments in agriculture began but this proto-agriculture appears to have been abandoned. Beginning around 10,500 BC stone sickles seem to simply fade out of the picture and there is a return to the hunter-gatherer culture.

Interestingly, these “industries” have associated cemeteries and evidence of ritual burial. In the cemeteries there are numerous bodies from the final thousands of years of the Upper Paleolithic that appear to have died violently. Stone points found with the remains were almost all located in areas of the body that suggests penetration as spear points or similar weapons. Most were located in the chest and back area, others in the lower abdomen, and a few entered the skull through the lower jaw or neck area. Additionally, the lack of bony calluses (which result with healing) shows that the wounds were fatal. In fact, it is estimated that 40 percent of the people died from wounds due to thrown projectiles - spears, darts, and arrows.

The cemeteries were used for several generations and many violent deaths occurred supporting the idea of massive inter-tribal warfare. The victims were of all ages, except infants, which indicates that the majority of the skirmishes were actually based on raiding and ambush, as "normal" warfare usually only involves young to middle-aged males.

We do not know the genesis of this warfare, only that it was intense. From other sources we do know that land and water were critical farming resources and have evidence from Lagesh and Umma (predecessors of Babylon) of “wars fought over the farming rights of shared land areas.” Sometimes called “the first war,” the Lagesh-Umma war was resolved through diplomatic means around 2500 BC. Mesilim, the King of Kish, is the author of a royal inscription, in which was recorded his arbitration of the boundary dispute between these cities. This idea of a “trusted third party” was understood and was in use at that early

Figure 7 - The Stelae of the Vultures.

time. [4, 8, 10]

We move to 5500 BC. Here, instead of several industries, we find that there are basically two, called the Sharmarkian and the Arkinian. It seems clear that these industries were significantly less sophisticated than their predecessors, indicating that "knowledge" was lost during this extended period of turbulence. It may be that the persons in whom the knowledge was vested were killed before the knowledge could be passed on[8].

We know that agriculture was begun 4000 years earlier and then abandoned, but we find a resurgence of farming between 6000 and 5000 BC. At this time we also find domestication of animals. As importantly, there is evidence that writing developed during this period which led to Old Egyptian that we find in the Unas tomb. There is also evidence of a large population explosion around this time (5500 BC).

A reasonable hypothesis is that warfare, loss of land, loss of technology, loss of knowledge, loss of life, and loss of history that we see in this scenario may well have led to understanding of the need to make permanent records of deeds, possessions, technologies and war plans, and to keep some of these from purview of enemies. A natural management position in cases of catastrophe, such as this, is to "ensure that it never happens again." Writing may have been a key to accomplishing this feat. [4]

Pre-Dynasty. About 5500 BC, a period that we call the Naqada III period, or Dynasty 0, represents formative years just prior to the unification of Egypt. It is a period in which ruling families appear to have controlled large segments of Egypt. These ruling families used recognizable royal iconography to express the ideological basis of their power and may therefore justifiably be called kings. Most of this iconography showed a relationship of the ruling family to the god Horus and it was this relationship from which authority was derived.

The iconography is clearly a seal of authority (a.k.a., signature) that we suspect was also used as a "mark of authenticity." This may also be the point in time when writing was finally used to communicate knowledge. We find stylized symbols and signs that conveyed information - including some short phrases.

[8] Knowledge commonly was vested in priests, shaman, astrologers, and other people who passed the knowledge to successors many times through family relationships. Knowledge was documented only through the minds of people and through verbal storytelling. Death of the "repositories" of knowledge could lead to loss of that knowledge.

Some bone and pottery vessels were inscribed (some in ink) with the figure of a scorpion which has been interpreted as the name of the owner. Different inscriptions bear common signs, and though we do not understand them, they are clearly communicating some commonly understood notion[9].

Figure 8 - The Scorpion King Mace head.

One of the best known artifacts from the period is the mace head of a king referred to as the Scorpion King[10]. The Scorpion King immediately precedes the first Egyptian Dynasty but we do not know a great deal about him. [8, 10]

There is good evidence to suggest that animal skins or masks may have been worn for various ceremonies and in battle, and many of the earliest kings appear to have associated their names with animals. Hence, scorpion may have been this king's true name, since it has been convincingly demonstrated that the rosette sign above the scorpion on this mace head signified the ruler. Regardless the notions of identification, authentication, and of ownership are evident of these inscriptions. [4]

First Dynasty. We now enter a near-historic era. The first dynasty, beginning about 2900 BC is the era in which the two parts of Egypt, upper and lower, were established under a single ruling family. It is also the time when we know for certain that the Egyptians and the Mesopotamians were in direct contact, though there is evidence of earlier contact. There is strong evidence of Mesopotamian influence in many of the artifacts found in the dynastic tombs. One of the outstanding accomplishments, even though no sentences could yet be

---

[9] Communication of a notion through symbols is common. It has been observed that the cliff paintings (petroglyphs) of Native Americans in the desert Southwest are written on stone. Many of these petroglyphs are messages along trade routes. Although few Native American tribal groups spoke each others' language, the petroglyphs are surprisingly standard throughout the desert and are understood across tribal groups.

In ancient Europe, important knowledge was preserved in the form of runes. Runes are symbols that are placed into a “layout” or position used for forecasting, magic, and communication. Some even suggest that such famous structures as the Henges (Stonehenge, Woodhenge) are runic in nature. These layouts are common across many areas of Europe.

Chinese, Japanese, Korean, Mongolian, and other languages of the Far East are ideographic. An ideograph, or character, represents an idea rather than a word. Some Chinese can read Japanese ideographs, and vice versa, without being able to speak the other language.

[10] The Scorpion King was made famous in a recent movie starring “The Rock” of professional wrestling fame.

written, is the use of “labels” indicating ownership, identity, and relationship[11]. [4, 8]

A very interesting example is the label NAR-MER, representing perhaps the second Pharaoh of united Egypt. The label appears as two syllabic figures between the cows' heads on the Kings cosmetic palette. [2, 10]

Figure 9 - The NAR-MER Pallette.

Second Dynasty. The second dynasty began about 2700 BC and is the era in which the step pyramids were built. This dynasty began dating objects. In this dynasty, there were apparently conflicts with the Libyans and those conquests were documented. It is characteristic of Egyptians that they were *always* victorious in battle with non-Egyptians - perhaps this is the first evidence of obfuscation of fact – a primitive operation that we might today call “confusion“. Regardless, labeling of data, dating of events, and obfuscation of events are primitive functions for cryptography. [4, 8]

Third Dynasty. The third dynasty, around 2600 BC, is the period of increasingly sophisticated pyramid building. A great deal of computational mathematics and measurement was developed in pursuit of perfection of the pyramids. This is the dynasty in which the great advances in mathematics, medicine, architecture and other sciences were developed. A key figure in this era was Imhotep who was probably “Egypt’s” equivalent of Leonardo Da Vinci[12]. Imhotep is credited with invention of building in stone (rather than brick), but was consulted on many matters of concern including medicine, mathematics, agriculture, and weather. Planning and the sophisticated use of heuristic reasoning are associated with this dynasty. [4, 8]

Fourth Dynasty. The fourth dynasty is the period around 2650 BC of the great pyramids built on the Giza plateau and elsewhere. These pyramids exhibit a technical genius that continues to stun people. The

---

[11] A very significant development in the history of writing, since the first development of a script in about 3100 BC, is the move from a pictographic or syllabic system to a phonetic one, based on the spoken sound of a word. This liberates writing from the status of an arcane skill, requiring years of study to learn large numbers of characters. It makes possible the ideal of a literate community. This step was not yet taken in Egypt, however.

[12] Imhotep was made famous in the recent “Mummy” movies but there is a great deal of evidence that his fame was much great and widespread even to the point of “deification.”

administrative capabilities needed to pull together these precisely oriented and persistent structures must be admired, and as we learn more about them, we continue to be impressed with the technology that must have been developed using rudimentary tools. While there are no "wall writings" in these pyramids, there were inscribed slate and carved figures and relief inscriptions that provide some information about the kings of the era. [4, 8]

Fifth Dynasty. We have finally made it to the dynasty in which Unas (or Unis or Wenis) was the final Pharaoh and where our journey will end. This is an era, around 2450 BC, in which the priesthood became extraordinarily powerful, perhaps exceeding the authority of the Pharaohs themselves.

The pyramid of Unas is smaller than that of any of his predecessors, but has been more fruitful in results of interest, the causeway, 730 yards long, is covered with relief of the finest quality. The subjects are very varied and unusual, illustrating, for example, the transport by ship from Aswan of granite date-palm columns and architraves used in the construction of the funerary temple. There are also scenes of workmen engaged in various crafts, and of people dying of hunger.

The internal arrangements of the pyramid are unusual, their main importance to Egyptologists lying in the fact that the walls of the vestibule and burial-chamber are covered with the oldest religious texts that have survived from Ancient Egypt, written in vertical columns. These texts contain spells providing for the welfare of the king in the hereafter. These are the first Pyramid Texts and are also found in the pyramids of four kings of Dynasty VI and elsewhere. [4, 8]

External Influences. We know that the ancient Egyptians interacted with other cultures in prehistory including Mesopotamia, Israel, Khatti, and Greece (Minoan Culture). It is not clear whether cryptographic primitives were Egyptian inventions or acquired from others. We suspect the answer is some combination of both.

Mesopotamia. Mesopotamian writing and cryptography apparently arose in an attempt to account for goods. A good example is provided by a tablet from about 1500 BC that contains an enciphered formula for making pottery glaze.

Figure 10 - A Mesopotamian Tablet with an Enciphered formula for making Pottery

Pictograms were used in the least common syllables to attempt to hide secrets of the formula. The method used is encoding rather than an

encipherment in which “objects” of a different sort are substituted for “known objects.” [7, 10]

Israel. An example of Hebrew cryptography is documented in the Bible (Torah) in Jeremiah that is called the ATBASH cipher from about 600 BC. The names of actual people and place names may well be enciphered in the Bible using the ATBASH to protect those people from various dangers.

Figure 11 - Substitution of Names of People and Places in the Bible.

The ATBASH cipher is a substitution cipher in which the order of the alphabet is reversed. In English, each A would be replaced by a Z, each B replaced by Y, each C replaced by X, and so on. One might note that this “permutation cipher” is actually congruent with reversal of columns in the Unas cipher, though letters are used in place of “pictographs” or hieroglyphs. The ATBASH cipher is a mono-alphabetic substitution cipher where the encryption is performed using a fully transposed or permuted (reversed) alphabet. [10]

Conclusion. The reader is, of course, free to draw his or her own conclusions, but we believe that we have provided evidence of the development of cryptography primitives in ancient Egyptian pre-history including:

- Functions (simple and composite)
- Transposition, Permutation, and Substitution
- Tagging, Labeling, Sealing, and Signing
- Authentication and Trusted Third Party
- Confidentiality
- Integrity
- Planning, Management, and Measurement
- Heuristics
- Keying
- Ownership

Postscript. We have surveyed some history, archeology, and cryptography and argued the merits of a plausible set of prehistoric developments that may well have led to the beginning of historical cryptography. Historical cryptography seems to begin with the tomb of the Egyptian nobleman Khnumhotep II. For interested readers, the historical story, beginning with Khnumhotep II to the present (with some gaps) we recommend the NSA Cryptologic Museum and of course David Kahn's book.

References

1. De Buck, Adrienne, The Book of the Two Ways, The Egyptian Coffin Texts, vol. 7 Texts of the Spells, Oriental Institution of the University of Chicago, 1961, pp 787-1185.

2. History of Writing, http://www.historian.net/hxwrite.htm

3. Pell, O, A Brief History of Cryptography and Cryptanalysis,

4. Shaw, I., The Oxford History of Ancient Egypt, Oxford University Press, 2000.

5. National Institutes of Standards and Technology, OECD Cryptography Principles, 1997.

6. Kahn D., The Codebreakers, Scribner; Rev Sub edition (December 5, 1996)

7. Saggs, H., The Babylonians, The Folio Society, 2003.

8. Gardiner, A., The Egyptians, The Folio Society, 2003.

9. Fraser, Sir James G., The Golden Bough, Macmillian, 1922.

10. Internet Sources:

- **www.thenagain.info**
- **www.wikipaedia.com**
- **www.touregypt.net**
- **www.fordham.edu**
- **www.nsa.gov/museum**
- **www.nist.gov**