CRYPTOGRAPHY DURING THE FRENCH AND AMERICAN WARS IN VIETNAM

PHAN DƯƠNG HIỆU AND NEAL KOBLITZ

Abstract. After Vietnam's Declaration of Independence on 2 September 1945, the country had to suffer through two long, brutal wars, first against the French and then against the Americans, before finally in 1975 becoming a unified country free of colonial domination. Our purpose is to examine the role of cryptography in those two wars. Despite the far greater technological resources of their opponents, the communications intelligence specialists of the Việt Minh, the National Liberation Front, and the Democratic Republic of Vietnam had considerable success in both protecting Vietnamese communications and acquiring tactical and strategic secrets from the enemy. Perhaps surprisingly, in both wars there was a balance between the sides. Generally speaking, cryptographic knowledge and protocol design were at a high level at the central commands, but deployment for tactical communications in the field was difficult, and there were many failures on all sides.

"Our friends...admired the determination and sacrifice coming from a small nation standing up against a colossal empire.... Our narrative was like the Biblical story of David against Goliath."

—Nguyễn Thị Bình (2013, p. 141-142)

1. Introduction

Does the history of cryptography during the French and American wars in Vietnam[1] have any relevance to the concerns of people working in information security in the 21st century? The years 1945–1975 predate public key cryptography, predate DES, and hugely predate the internet. Nevertheless, there are several reasons why this story needs to be told in our time.

In the first place, the victories — shocking and unexpected to many in the West — of a technologically backward people over two advanced industrialized Western countries were signature events of the 20th century. The humiliation of the French at Điện Biên Phủ in the spring of 1954 marked the beginning of the end of French colonialism; it was an inspiration to others, mainly in northern Africa, who were suffering under the yoke of French colonialism and who managed to achieve independence a few years later. Similarly, the expulsion of American forces from southern Vietnam on 30

Date: 8 December 2016; revised 6 February 2016.

Key words and phrases. wars in Vietnam, signals intelligence, communications security.

[1]This paper is a much expanded version of the second author's invited talk on 7 December 2016 at Asiacrypt 2016 in Hanoi, Vietnam.

April 1975 — which was the only time the United States has ever been decisively defeated in a war — gave tremendous encouragement to others, especially in Latin America, who were struggling against U.S. hegemony.

A common explanation for the Vietnamese victories is that the Vietnamese benefited from a two-millenia tradition — going back to the rebellion against Chinese domination led by the Trưng Sisters in 40 A.D. — of resisting foreign invasion and occupation. The tremendous sacrifices the people were willing to make to defend their land, combined with the sophisticated strategic thinking of such leaders as Hồ Chí Minh and Võ Nguyên Giáp, enabled the Vietnamese to overcome much more powerful and technologically advanced military machines.

Given this analysis, one might think that if we looked at the technological side of warfare — and, in particular, at communications intelligence — we would find that the Việt Minh (the name of the front that fought for independence from the French), the National Liberation Front (NLF), and the Democratic Republic of Vietnam (DRVN) must have been consistently outmatched and outclassed by French and American expertise and equipment. However, the truth of the matter is much more complex. During both the French and American wars, as we shall see, there was a surprising symmetry between the adversaries in both signals intelligence (SIGINT) and communications security (COMSEC). There were dramatic successes and major failures on all sides.

Perhaps the lesson to be drawn is that in SIGINT and COMSEC during the colonial wars in Indochina the human element was primary, and the technical element was secondary. Is this any less true of today's applications of cryptography? Indeed, if one can extract a single short message from Ross Anderson's thousand-page classic *Security Engineering* (Anderson 2008), it is that the human factor is just as central to cybersecurity in the internet age as it was to communications security during the wars of earlier times.

A second reason to be interested in history is that it should teach us humility. The need for this quality in order to make intellectual and scientific progress was well understood in ancient times. In Chapter 13, Verses 8-12 of the *Bhagavad Gita* we read that of the qualities that are necessary for knowledge the very first is *Amaanitvam*, the Sanskrit word for humility. Unfortunately, in our era of self-promotion and hype, in our frenetic rush to get grants and get papers published, many scientific research communities — including ours — often forget this lesson of history and need to be reminded. History sometimes plays cruel tricks on cryptographers who over-estimate their own cleverness.

There is a third sense in which the story of cryptography in Vietnam during the wars has relevance to us today. One of the motivations for many researchers in our field is the belief that cryptography has great potential to defend the "little guy" — the ordinary person — against powerful government agencies and giant corporations. This is certainly the viewpoint of such pioneers of modern cryptography as Whit Diffie and David Chaum,

and we can see it as well in the work of Phil Zimmerman (inventor of Pretty Good Privacy) and John Gilmore (a founder of the Electronic Frontier Foundation). From this optimistic point of view, crypto can be like the slingshot that the boy David used to take down the giant Goliath. And as pointed out in the above quotation of Nguyễn Thị Bình (who headed the delegation of the Provisional Revolutionary Government of South Vietnam at the Paris Peace Talks of 1969–1973), there are no better examples of a modern David-and-Goliath battle than the wars in Vietnam against the French and then the Americans.

FIGURE 1. Nguyễn Thị Bình at the Paris Peace Talks in 1969.

Finally, there is a fourth reason to be interested in this story. Modern cryptography has been U.S.-dominated, and many countries just follow the U.S. and import their cryptography from the West. This is regrettable. The Edward Snowden documents show the danger in doing this, and the need to have independent expertise and commercial development in crypto in other parts of the world. Thus, it is useful to study the strong cryptographic traditions from earlier times that exist in different regions of the world, such as Asia. Awareness of this history can give people in developing countries today the confidence needed to break free of a nearly total dependence on imported knowledge and imported products.

2. The French War (1945–1954) and the Inter-War Period (1954–1960)

2.1. **The early years.** From the beginning the leadership in Hanoi attached great importance to communications intelligence. According to a history by the Vietnamese government that was translated by the NSA (NSA 2014), the People's Armed Forces cryptographic branch was formed on 12 September 1945, just ten days after the Declaration of Independence of Vietnam.

At that time the cryptographic level of the Vietnamese was not high. As described in the Cryptographic Bureau's history (Ban Cơ Yếu n.d.), the

system they were using in late 1945 and early 1946 was little more than a Caesar cipher. More precisely, they would first regard the Vietnamese text as letters in a largely Latin alphabet, that is, drop the accents and merge some letters such as a, â, ă (which are distinct letters in Vietnamese). Then they would number the letters and shift the numbers by a fixed amount (in the illustrative example (Ban Cơ Yếu n.d.) the Caesar key is 10). The sequence of decimal numbers would be the ciphertext.

Then on 10 April 1946, the department heads were ordered to use a better, though still rudimentary, double encryption system. First, they would encode the different letters and accents using combinations of Latin letters; for example, "Lê Thái" would become *LEETHAIS*. Then they would convert to numbers using a fixed random permutation of the numbers 0 through 22 (three letters of the Latin alphabet were not used). Finally, they would encrypt the decimal digits with a Vigenère key of length 5 (that is, a 5-digit decimal number). The message digits would be divided into blocks of length 5, and the key would be added digit by digit modulo 10.

This system is very weak in comparison with state-of-the-art cryptography in 1946 and also in comparison with the systems used by the Vietnamese during the American war. The second layer of encryption can easily be stripped away; it compares unfavorably to ordinary Vigenère encryption with a 5-letter key, for which key recovery through frequency analysis would require one to examine a fair amount of ciphertext. In the first place, there is ambiguity in decryption by the recipient, because after inverting the Vigenère step the digits 211 could be read as either 2 11 or 21 1. More seriously, frequency analysis would be even easier than for standard Vigenère, because in each position (after the permutation step and before the Vigenère step) one would expect 1 to occur by far the most frequently and 2 to occur the second-most frequently.

One conclusion that can be drawn from the amateurish nature of Vietnamese cryptography in 1946 is that the Việt Minh had received no substantial assistance in this area from the Americans during the brief period when they were allied in the campaign to expel the Japanese. In early 1945 the U.S. Office of Strategic Services (the precursor to the CIA) sent a team, led by Col. Archimedes Patti, to work with the Việt Minh to set up an intelligence network to report on Japanese movements (Patti 1981). Col. Patti met with Hồ Chí Minh and Võ Nguyên Giáp, and got their full cooperation. The Americans quickly got a large amount of tactical information that the allies used against the Japanese. One might have expected that part of setting up the intelligence-gathering project would have been to teach some basic cryptography to the Việt Minh. If that had happened, then presumably the Vietnamese would have been farther along when they set up the cryptographic branch a few months later. But apparently the Americans helped the Việt Minh much less than the Việt Minh helped them.

From the interview (Patti 1981) one can see that there were geopolitical reasons why the Americans would not have been likely to give help in

cryptography to the Việt Minh. The U.S. side wanted just a temporary alliance until the Japanese were defeated. Patti's superiors had expected that the Việt Minh would simply ask for money in exchange for supplying information on Japanese movements, and they were ready to oblige. They were very surprised when Patti told them that the Việt Minh were happy to help the Americans without being paid for it. On the Vietnamese side, Hồ Chí Minh wanted a long-term alliance with the Americans against the French, and he was encouraged by the fact that in 1945 the U.S. was formally neutral (the orders to Patti were not to help the French return, but not to directly oppose them either). Basically, the Việt Minh gave a lot of help to the Americans in the hope that the Americans would support independence for Vietnam. Of course, later the Americans betrayed them and supported the French; by the end of the French war in 1954 the successor organization to the OSS — the CIA — was flying supplies to French forces at Điện Biên Phủ. In 1945 the U.S. was gearing up for the Cold War, and under those circumstances it was unlikely that the U.S. would have given cryptographic help to a communist-led group.

In this early period the cryptographic weakness of the Việt Minh resulted in the loss of secrets to the French. At the Franco-Vietnamese Conference in Fontainebleau in July–August 1946 (which failed to produce a peace agreement), the French were able to read some weakly encrypted Vietnamese diplomatic messages. Around the same time the French had similar success at a conference held in Đà Lạt. According to Christopher Goscha (2012, p. 813), a prominent expert on the French war,

> Reliance on radio communications also carried serious risks. The French had already sent some of their best code breakers to Indochina so they could inform local and metropolitan French leaders what the other side was saying behind closed doors. Vietnamese efforts at modern diplomacy were hampered on the technological front by their lack of sufficient encryption techniques, equipment, or training. This was particularly true at the beginning of the war, when Vietnamese encryption methods and tables were crude, and inexperienced radio operators too often grew frustrated and simply sent their messages un-coded. As a result, the French were able to read much of the DRV[N]'s cable traffic during the Đà Lạt conference and also, it seems, during the one at Fontainebleau.

However, the Vietnamese were working hard to improve their cryptographic knowledge. They studied the book *Eléments de cryptographie* by Captain Roger Baudouin, a comprehensive textbook published in Paris in 1939. In 1948 the Việt Minh published a training manual for cryptographers, which was widely used during the French war. Written by Hoàng

Thành and titled *Foundations of Cryptography* (Mật mã đại cương), it is currently on display in the Cryptographic Museum in Hanoi.

There is some evidence that the growing cryptographic sophistication of the Việt Minh center did not necessarily extend to their cadres in the field. A fascinating exhibit in the Hanoi Police Museum depicts an action of Việt Minh commandos who blew up the French ship Amyot d'Inville on 27 September 1950, thereby thwarting a major French attack on the Thanh Hoá – Nghệ An – Hà Tĩnh liberated zone of central Vietnam. The exhibit includes the original instruction sheets describing the cryptography they used. The instructions explain how to use a Vigenère cipher with key-length 5. The keyword TINHA is displayed at the top of a table with the shifted alphabets below. A 17-letter sample message is padded with OOO and then divided into four 5-letter blocks and encrypted. The resulting ciphertext is highlighted in a rectangular box. But alas! The first block of the transmitted ciphertext is the keyword! And everything is nicely spaced so as to leave no uncertainty about keyword length. At least they didn't have any problem of key distribution!

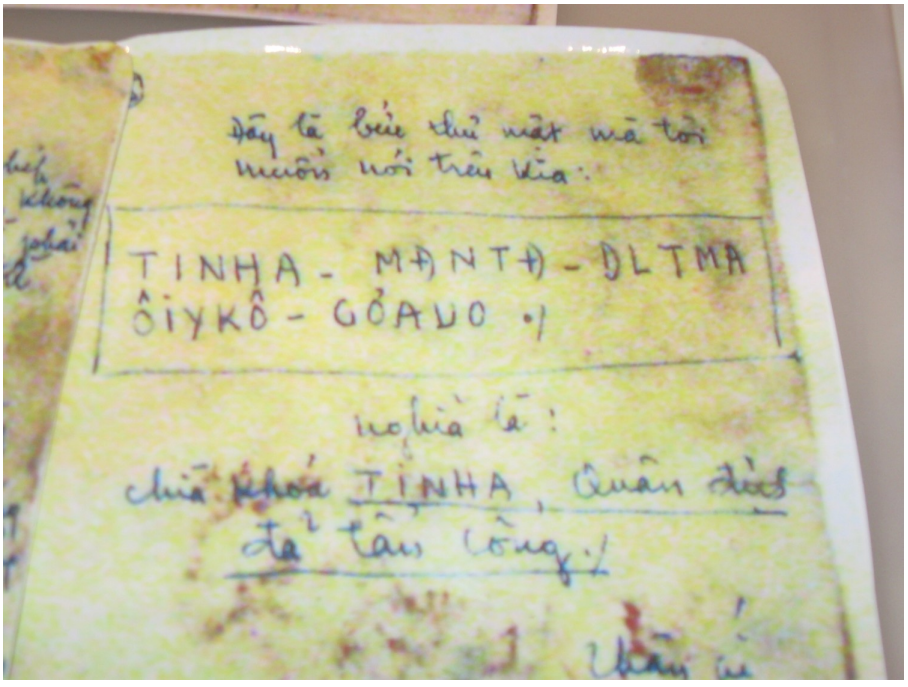

FIGURE 2. The keyword TINHA is the first block of ciphertext.

But before we laugh at their blatant violation of Kerckhoffs' principle, we have to acknowledge that their attack on the French was one of the great successes of a secret guerrilla cell during that epoch.

Why didn't their poor use of cryptography lead to discovery and defeat? Perhaps the French never captured any of their communications, so they

could have equally well just sent the plaintext. Or perhaps the French did capture something, but were too ignorant of cryptography even to crack a Vigenère cipher when given the key. Most likely both the Vietnamese commandos and the local French enemy were so isolated that they could not benefit from whatever cryptographic knowledge was in the respective command centers.

2.2. **The role of the USSR and China.** In any case, according to the history (NSA 2014), just a few months later, in November 1950, the Vietnamese sent their cryptographers to China for six months of training that greatly improved their technical level. For the Vietnamese at this time, the Chinese experience provided a tremendous model of revolutionary struggle; just the year before the Chinese communists had defeated a Western-supported regime in an epic guerrilla war.

However, in communications there was an important difference. The Chinese had to first translate or transliterate to a standard alphabet before encryption. But Vietnamese is written in a modified Latin alphabet, and so can be encrypted directly, provided that some alterations are made. As described in "Vietnam: A SIGINT Paradox" (NSA 2007),

> Vietnamese cannot be transmitted by using standard international Morse code because of its peculiar letters and use of accent marks. The [NSA] cryptolinguists had to learn the system created by the Vietnamese to express these features in Morse before tackling an actual translation. For instance, the vowels u and o appear as simple letters or with hooks. To indicate the use of the letter u with a hook, the Vietnamese operator sent the letters uw. W does not exist in the Vietnamese alphabet so it was available for special assignment.

The article goes on to say that because ươ occurs so often, the Vietnamese Morse code operators would shorten uwow to simply wow.

In the 1950s the main foreign help in communications security came from China. In the late 1950s the Soviet Union started to replace China as a source of cryptologic advice, although China continued to assist Vietnam in other areas, especially in air defense. According to U.S. intelligence estimates (Hanyok 2002, p. 261), between 1965 and 1973 over 5000 Chinese advisers were killed or wounded by the U.S. Air Force attacks on northern Vietnam. USAF General Curtis LeMay famously said that he wanted to "bomb them [the Vietnamese] back into the Stone Age," and even foreign advisers assisting Vietnam often fell victim to the carpet-bombing.

Retired CIA Vietnamese language expert Merle Pribbenow (2014) describes the history of Soviet assistance to Vietnam in intelligence. In response to a request from Hanoi, in 1959–1961 the Soviet State Security Committee (KGB) supplied funding, equipment, and training in radio intelligence and secure communications. This ambitious and successful project was called "Vostok" in Russian ("East") and "Phương Đông" in Vietnamese.

Pribbenow writes that the KGB provided "equipment and technical support to the Ministry of Public Security for the establishment of a massive secure communications network throughout North Vietnam, and indeed extending down into South Vietnam to support the war effort there."

As the title of Pribbenow's article suggests, there was some tension in the relations between Vietnam and both the USSR and China, largely caused by the Sino-Soviet dispute that became increasingly bitter during the 1960s. Under Hồ Chí Minh's leadership the Vietnamese tried hard to navigate a middle course between the two superpowers. It was not easy, as both the USSR and China on occasion tried to use Vietnam as a pawn in their rivalry. During the Cultural Revolution in China, some Red Guard units even blocked trains that were carrying Soviet military aid in transit through China to Vietnam. But the Soviets could cause problems, too, by exploiting internal disagreements in the Vietnamese Communist Party in an attempt to move the Party toward an anti-China stance. Hồ Chí Minh firmly believed that such a move would not be in Vietnam's best interest.

According to Pribbenow (2014), the tension and mistrust in both the Vietnam–USSR alliance and the Vietnam–China alliance caused the Vietnamese to avoid becoming dependent on either nation for their cryptography. Much of the time they used their own ideas and materials, and this in fact made the work of the French and American cryptanalysts more difficult. By the latter part of the French war, Vietnamese cryptography — and, more generally, their use of communications technology — was at a surprisingly high level for a guerrilla army in an impoverished country. According to Goscha (2012, pp. 829-830):

> It is clear that the DRV[N] did not just overwhelm the French with big guns and waves of attacking men; a key reason for the victory [at Điện Biên Phủ] was their success in organizing and executing a highly complex battle, which in turn relied on their ability to control space and time via the airwaves. Nowhere in the twentieth century history of the wars of decolonization in the non-Western world has the technological organization of such a modern battle been duplicated. Neither the Front de libération nationale (FLN) fighting the French for Algeria nor the Republicans battling the Dutch for Indonesia ever used communications so intensely to both drive state-making and take the fight to the colonizer on the modern battlefield.
>
> It was clear from their technological accomplishments that the DRV[N] was by the end of the conflict no longer a ragtag team of guerrillas, running low intensity, haphazard hit-and-run operations, at least not in the north. Nor was the DRV[N] state acephalous and disconnected; though the DRV[N] state was in many ways still rough, erratic, and fragmented,

> communications gave it form both militarily and institutionally. The French broke scores of Vietnamese codes and arrested thousands of couriers, but they were never able to stop their adversary from communicating vertically and horizontally. This study of the DRV[N]s communication and information networks has offered a unique take on how this state forged in war linked itself and its army across time and space by circulating information essential to its survival, institutionalization, national legitimacy, and hold on power.

By the beginning of the American war, U.S. cryptographers had a high estimation of the cryptographic level of their adversaries. The declassified history (NSA 2007) concludes, "In 1961...NSA analysts knew that our opponents were good at the cryptologic trade and maintained a healthy respect for the cryptologic abilities of the North Vietnamese."

2.3. **French cryptography in Vietnam (1945–1954).** Judging from sources in the French military archives, French cryptography during this period had similarities to Việt Minh cryptography. Although the French used some relatively advanced equipment, such as the M-209 that had been developed by the U.S. during World War II, in practice they were on roughly the same level as their opponents; both sides were plagued by problems of poor training and misuse of their respective systems.

Like the Việt Minh's cryptography, the French systems were essentially variants of the Vigenère cipher. In the early years of the war French secret communications were often captured and decrypted (if, in fact, they had been encrypted at all), but by the end of the war their communications security had improved.

The irony is that Blaise de Vigenère was a Frenchman who in the 16th century made major advances in cryptography. At first glance it would seem that the French had made no progress in that field in 400 years. But their real problem was that theoretical knowledge would not carry over to practice, at least not in Vietnam, for three reasons. First of all, in the mid-20th century Vietnam was a remote outpost in the French empire. Hanoi was very far from Paris in every conceivable sense. Moreover, although early in the war France did send some well-trained cryptanalysts to break Vietnamese diplomatic communications, for the most part it was not France's most intelligent citizens who were sent to Vietnam to combat the independence movement.

In the second place, in the years before the computer strong encryption was very slow. A document from the military archives dated 7 December 1953 — just three months before the Battle of Điện Biên Phủ — reported on an experiment comparing the time needed to encrypt a message using six different encryption schemes. The slowest took 44 minutes, and the fastest took 17 minutes. The conclusion was that the fastest encryption scheme

should be used. Note that the recommendation was based on a comparison of speed, not a comparison of security.

In the third place, human error and reluctance to follow the rules bedeviled the French authorities. A document dated 11 December 1953 (General Babet's End of Mission Report, Centre historique des archives) complains about "indiscrétions" and "fautes graves contre ces regles" that had led, among other things, to a recent "coup de main" by the Việt Minh.

The French military commanders acknowledged that in general the most they could hope for was to get their officers to use a very weak encryption. They even introduced a term for that, *camouflé* ("camouflaged"), meaning halfway between plaintext and ciphertext. True encryption was used only for short, top secret documents.

3. The American War (1961-1975)

In studying the history of cryptography in a war one must distinguish among different types of questions:

• Offense (SIGINT). What was the level of signals intelligence on all sides? To what extent were they able to benefit from intercepted communications of their adversaries?

• Defense (COMSEC). What was the level of cryptographic knowledge and practice on all sides?

• Strategic communications, which took place between command centers and major bases and were generally not very time-sensitive. How secure were the strategic communications of the different sides in the wars?

• Tactical communications, including real-time battlefield communications and preparations for battle. How secure were they?

3.1. **U.S. COMSEC vs Vietnamese SIGINT.** Brian Snow started to work at the NSA in 1972, and eventually rose to be Technical Director of COMSEC (which at the NSA was later called the Information Assurance Directorate, IAD). In responding to questions about NSA policy on COMSEC during the war in Vietnam (Snow 2015), he stressed that IAD always used a worst-case — never a probable-case — analysis. They would not have made the mistake of underestimating Vietnamese cryptanalytic skills. Even without any confirmation that the Soviet Union or China was giving substantial help in cryptanalysis or that the Vietnamese on their own had developed high-level capabilities in SIGINT, the COMSEC people at the NSA would always assume the "worst," and would insist from the beginning that the U.S. military use advanced cryptographic protection. This worked fine for strategic communications; the Vietnamese were never able to penetrate the strong encryption that the NSA provided.

FIGURE 3. The NSA's NESTOR encryption device.

3.1.1. *The tactical dilemma.* In about 1965 the U.S. started deploying an encryption device called NESTOR that had been developed by the NSA for battlefield use. However, NESTOR worked badly in the heat and humidity of southern Vietnam. In practice, most American battlefield communications were unencrypted or were informally encoded using jargon, ad hoc word and phrase substitutions, etc. Although many in the U.S. military believed that the Vietnamese would never be able to understand American jargon and informal codes in real time, in reality the NLF was often able to exploit insecure tactical communications by the U.S. military.

In a 1982 book by U.S. Army Lt. Gen. Charles R. Myer (the cryptographic sections were reprinted in *Cryptologia* (Myer 1989)), he tells of a raid on an NLF installation on 20 December 1969 that resulted in the capture of 12 cadres and large quantities of documents and communications equipment. By examining the equipment and "interrogating" (Myer's word) the prisoners, the U.S. learned that with the help of "English linguists [who were] an integral part of Viet Cong and North Vietnamese units," they could "monitor and exploit virtually all nonsecure voice and manual Morse code communications." Captured documents contained "extensive instructions on proper intercept techniques and detailed analyses of the communications procedures and exploitable weaknesses of U.S. and allied units."

When Gen. Creighton Abrams, commander of all U.S. forces in Vietnam, was briefed on this, he stated, "This work is really rather startling; the attention to detail, complete accuracy, and thorough professionalism is amazing. These guys are reading our mail, and everyone will be informed that they are." But despite the efforts of the command to get U.S. troops in the field

to use strong security for tactical communications, they continued to be very resistant, in part because of the tremendous difficulties they had with the KY-8, KY-28 and KY-38 NESTOR encryption devices. Myer concludes:

> Signal security, particularly in voice radio transmissions, was a major problem area throughout the period of combat operations in Vietnam.... All users of communications facilities were more or less aware of their vulnerability to enemy intercept, analysis, and decoding, and of the need for authentication and encoding. The gap between this knowledge and actual practice was immense, and in Vietnam it seemed at times an insurmountable problem.

Concerning the need for authentication, Myer explains that there were "numerous instances on record" of the NLF sending false messages. "In one case the enemy tapped the internal telephone lines of a defensive base and diverted reserve forces from the area where he [the NLF] attacked."

Myer also tells of a case when a U.S. operator removed the cover of a KY-8 NESTOR to allow ventilation and cooling (since overheating was the biggest problem with these devices). "That improved the operation of the KY-8 but violated security by exposing the equipment to view and giving the enemy an opportunity to intercept intelligible signals." The suggestion that the NLF was probably able to take advantage of a side channel in the NESTOR is "startling," to use Gen. Abrams' word. Imagine a half-century ago, in a guerrilla encampment hidden deep in the hot and humid jungles of southern Vietnam, an NLF SIGINT unit exploiting side-channel vulnerability of an NSA encryption device, and listening in on supposedly encrypted U.S. tactical communications!

3.1.2. *Human intelligence.* As mentioned above, the Vietnamese were not able to cryptanalyze the strong encryption that the U.S./RVN used for strategic communications. (RVN stands for Republic of Vietnam, the name of the regime in the south that remained in power because of the American occupation.) Rather, the Vietnamese circumvented the whole problem by having a large network of secret agents with access to key sources of strategic and tactical information in the RVN military and security services, and even in the U.S. intelligence services, especially the CIA.

3.1.3. *Phạm Xuân Ẩn (1927–2006).* After World War II the United States emerged as the superpower opponent not only of the Soviet Union, but also of left-led liberation struggles around the world. In particular, by the early 1950s the U.S. was heavily involved in supporting the French in Vietnam with money and matériel. The leaders in Hanoi anticipated that once they defeated the French, they would have to deal with the Americans, who would not sit idly by and allow the unification of Vietnam under communist leadership. To be sure, the Geneva Accords of 1954 provided for nationwide elections to be held in 1956 to determine the composition of the government

of a unified Vietnam. However, U.S. intelligence estimated that in such an election Hồ Chí Minh would win 80% of the popular vote (Eisenhower 1965). The elections were never held.

Although in 1946 Hồ Chí Minh had appealed to U.S. President Truman for support for Vietnamese independence, by the early 1950s the Vietnamese leadership was not so naive as to think that the U.S. would allow them to unify the country through elections. Rather, they knew that they had to expect the French war to be followed by an American war. They decided that it would be invaluable to prepare for this by having a highly-placed source of accurate information on American strategic and tactical thinking. They chose the young Việt Minh sympathizer Phạm Xuân Ẩn for this task. Ẩn became the most famous spy in the history of Vietnam.

In 1953 Phạm Xuân Ẩn was inducted into the Communist Party of Vietnam by Lê Đức Thọ (who twenty years later was offered the Nobel Peace Prize along with Henry Kissinger for negotiating the Paris peace agreement; Thọ declined the prize). Ẩn was told to refrain from any activities that would identify him as pro-communist. In 1957 Ẩn was sent to the United States to study journalism, after which he went to Saigon as a key figure for the U.S. news media, especially during the crucial years of the war, when he worked for *Time* magazine. He was trusted by top CIA people as well as by key officials of the South Vietnam regime.

Ẩn's career as a deep mole working for NLF and DRVN intelligence lasted 15 years, from 1960 to 1975. In secret he received sixteen medals for extraordinary service. On one occasion, after receiving Ẩn's reports, General Võ Nguyên Giáp and President Hồ Chí Minh said, "Now we are in the Americans' war room." After the war, in 1976 Ẩn was named "Hero of the People's Armed Forces of Vietnam." He later rose to the rank of Major General, and when he died in 2006 he was given a war hero's funeral. For more details about his life, see the two books in English (Berman 2007, Bass 2009), which make the case that he was possibly the most masterful and successful spy of the twentieth century in any country.

We will return to the story of Phạm Xuân Ẩn when we discuss Vietnamese encryption.

3.1.4. *Nguyễn Đình Ngọc (1932–2006).* Ngọc was a mathematician who worked under cover in Saigon and also rose to the rank of Major General (in his case this was a police rank, not a military one). He had several math and engineering degrees (all from France). In the 1980s he helped organize seminars in algebra, topology, and other areas. He was also a friend of the families of both authors.

During the American war Ngọc, who was fluent in English as well as French (in 1983 he translated the first public talk in English that the second author gave in Vietnam), circulated widely in the foreign community in Saigon and acquired valuable intelligence from them. He also had a brother

FIGURE 4. Photo on left: Phạm Xuân Ẩn (right) with General Võ Nguyên Giáp; photo on right: Nguyễn Đình Ngọc.

who had a high rank in the RVN military. We do not know whether Ngọc used his mathematical and engineering knowledge to strengthen Vietnamese cryptography. It is not even clear that he encrypted his own reports. One source (Phượng 2016) has suggested that he probably had a personal contact in Saigon (another spy) to whom he gave his reports orally, and then that person was responsible for transmitting them to Hanoi.

There were many, many other human intelligence sources working for the NLF and the DRVN. For the Vietnamese the main method for strategic intelligence gathering was through their extensive network of undercover agents, not through any cryptanalysis of the high-level ciphers that the U.S. used for strategic communications.

3.2. **Vietnamese COMSEC vs U.S. SIGINT.**

3.2.1. *Vietnamese encryption.* Merle Pribbenow, who wrote the report (Pribbenow 2014) cited above, retired in 1995 after 27 years working for the CIA as a Vietnamese language specialist. In an email (Pribbenow 2016b) he summarized the state of Vietnamese encryption during the American war as follows:

> North Vietnam sent cryptographers and radio operators south ... in the early 1960s ... to upgrade the security of their communications with the South. The Vietnamese used several different systems during the course of the war, and upgraded their encryption systems several times. By the end of the war at least they were using a double encryption system, involving the use of substitution codes from a code book and then enciphering the coded message using a one-time pad.

In a follow-up telephone conversation he added: "The Vietnamese used both Morse code and voice for ciphertext, reading Vietnamese words by radio to stand for letters, much like the U.S. military's use of Alpha, Bravo, Charlie,... for A,B,C,...."

A visit to the Cryptographic Museum in Hanoi provided some details. The Vietnamese moved through three general techniques during the three decades of war, denoted KTA, KTB, and KTC (here KT is the abbreviation of the Vietnamese word for "technique"). KTA was a conventional encryption scheme based on permutation and substitution, whereas the different variants of KTB and KTC involved some kind of double encryption. By the start of the American war KTC was being used; by the end of the war the Vietnamese were using KTC-5, where the 5 indicates the block length.

In the first stage of KTC-5 a word was encoded by dictionary look-up; a copy of such a dictionary is on display in the museum. A dictionary would be shared by many users, and when one was captured by the U.S., a new one would be issued immediately. In the second stage the encoding was encrypted using a one-time pad. This was a book, shared by only two users, that was printed in very small type, requiring a magnifying glass to read. The tiny book could be easily destroyed when there was a danger of capture. Printing these books was beyond the capability of Vietnamese presses, and so it was done in the Soviet Union.

The dictionary look-up method is especially suited for Vietnamese, because in Vietnamese all words naturally subdivide into component one-syllable words. For example, the word "attack" in Vietnamese is *tấn công*. The first step, using the dictionary that's on display in the Cryptographic Museum, is to map *tấn* to the block **afhbv** and *công* to the block **wxess**, resulting in a 10-letter encoding for "attack," which is then encrypted using a one-time pad.

From our sources[2] it is clear that the U.S. never could read KTC-encrypted traffic.

3.2.2. *Invisible ink, and some questions.* During the years 1960–1975, when Phạm Xuân Ẩn was sending secret information from top U.S. and RVN sources, out of a total of 45 couriers employed for his messages 27 were captured and killed — and presumably tortured before they were killed. Yet the enemy never learned who the source of those messages was. At first one would think that this meant that all of his messages must have been strongly encrypted. However, we learned that, because Vietnam's strong encryption was a slow and lengthy process, this was not the case.

According to our sources (Berman 2007, Bass 2009, Tư Cang 2016, Phượng 2016), what typically happened was the following. Ẩn would write his reports in rice-starch invisible ink on paper which he would then wrap around egg rolls. In a market he would give the egg rolls to his first courier, a woman by the name of Nguyễn Thị Ba, who also survived the war and in

[2]Pribbenow (2016a) said this directly, and one can also surmise this from the fact that the different NSA sources (Johnson 1995, Hanyok 2002, NSA 2007, Borrmann et al. 2013), while describing U.S. intelligence successes from traffic analysis, direction-finding, and interception of unencrypted and weakly encrypted communications, mention nothing about breaking Vietnam's strong encryption.

1976 was named "Hero of the People's Armed Forces of Vietnam." Couriers would take the messages to the NLF center in the tunnels of Củ Chi, not far from Saigon. There NLF intelligence would apply an iodine-alcohol solution to make the ink visible, and then rewrite the text in invisible ink in two sections. One section would be a relatively short time-sensitive report; the other would consist of longer, less urgent reports. The first part would be carried to a broadcast installation and sent by strongly encrypted radio link to NLF headquarters in Cambodia. The second section would be carried on foot to the Vietnamese leaders in Hanoi.

This leads to an interesting question. Why was U.S. and RVN intelligence unable to determine the source of the unencrypted reports of the captured couriers? Could they have been unaware that the NLF was sending messages in invisible ink? On the contrary, according to Pribbenow (2016b), "The CIA and the South Vietnamese were well aware that the Vietnamese communists sent messages by courier using secret writing (invisible ink) and that these messages were usually unencrypted. The French had similarly been aware of the same thing during their earlier war against the Việt Minh."

One possible answer to this mystery (Phượng 2016) is that the couriers could easily destroy the messages in various ways when they were on the verge of capture. This is a partial explanation. However, the year, location, and circumstances of capture of the couriers varied considerably, and it is hard to believe that in all 27 cases they were able to totally destroy the messages.

Another explanation might be that the first, highly sensitive section of the message perhaps was never captured. That was the part that was carried on foot only as far as Củ Chi and a nearby radio transmitter. The second part of the message was of a nature that was less likely to point toward a particular source — gossip about conflicts and changes within the RVN political and military establishment, general assessments and planning by the Americans, tensions in U.S.-RVN relations, political and military vulnerabilities, and so on. Such information could have been traced to many different possible sources, and U.S. intelligence was well aware that the RVN military and intelligence services were riddled with spies.

3.2.3. *The tactical dilemma.* According to Pribbenow (2016a), the NSA and the cryptographic branches of the Army, Navy, and Air Force never broke any of the high-level ciphers that the Vietnamese used for strategic communications. However, the Vietnamese tactical communications were either unencrypted or weakly encrypted and easy for the NSA to read.

The problem for the Vietnamese was that encryption was very slow, and so could not be used if either (1) a vast amount of information had to be sent, as, for example, in 1967–1968 when personnel and matériel were moving south in preparation for the Tết Offensive, or (2) information had to be sent extremely fast, as in the case of air defense. The NSA history (Hanyok 2002, Chapters 6 and 7) describes two key areas where SIGINT gave the

Americans tactical benefits. First, starting in 1967, they were able to accurately estimate the numbers and destinations of liberation forces moving south on the Hồ Chí Minh trail. At the same time SIGINT traffic analysis was able to give the Americans a tremendous tactical advantage in the major battles in the Central Highlands that were preliminary to the Tết Offensive, notably the battle of Đắk Tô that lasted through most of November (Borrmann et al. 2013, pp. 40-42). (Actually, NSA officials claimed that, starting about two years earlier, they had been able to predict the date, target, and attacking units for most major NLF offensives through a combination of direction-finding and painstaking traffic analysis (Hanyok 2002, p. 539).)

Second, during the air war, signal intercept operators were often able to alert U.S. bombers about threats from North Vietnam's air defense. By the late 1960s that air defense was a formidable network of air warning and tracking stations (visual and radar), anti-aircraft artillery (AAA) and surface-to-air missile (SAM) stations, and MiG's. A complex web of communications had to be coordinated through the air defense headquarters at Bach Mai Airfield in Hanoi. As explained in the NSA history (Hanyok 2002, p. 237), "most messages passing over the communications system used low-grade encryption or encoding systems or were in plain language. This latter situation was due to the need for getting information quickly through the air defense system." By the later years of the air war, U.S. SIGINT had become very efficient at analyzing Hanoi's air defense communications and using that data to help American bombers get through. Vietnam did manage to shoot down many U.S. bombers. But they would have destroyed many more if they had been able to encrypt their air defense communications. Unfortunately, this was impossible.

During the Tết Offensive and during the air war, American SIGINT allowed the U.S. to inflict greater casualties and suffering, but of course this did not alter the outcome of the war.

3.3. **Conclusion: A surprising symmetry.** In the Introduction we commented that a common view of the American war in Vietnam is that, despite overwhelming technological superiority, the Americans lost the war because the "hearts and minds" of the people were on the side of their opponents. In view of the assumed vast technological inferiority of the Vietnamese, it is somewhat surprising that in a crucial realm of military technology — communications security and signals intelligence — there was a type of symmetry between the two sides. In both cases COMSEC worked well for strategic communications, but was woefully inadequate for tactical communications. The Vietnamese had, on balance, successes and failures that were similar to those of the Americans.

The Americans' NESTOR encryption devices were well constructed to achieve the desired cryptographic functionality; they worked fine when tested at Fort Meade. But they worked poorly in the heat and humidity of southern Vietnam. The Vietnamese double encryption system was well designed and,

it seems, was never broken. But it was too slow for tactical communications that had to be encrypted and decrypted in real time, and it could not be used to send large volumes of information.

We have also seen how the human element so often stands in the way of good communications security — the smug self-confidence of local American commanders who thought that the NLF linguists would never be able to understand American military jargon and informal codewords, the naïveté of the Việt Minh commandos who happily included the keyword as the first block of ciphertext. In retrospect, the huge disparity between the level of cryptographic knowledge at the command centers and the realities of tactical deployment in the field should not have surprised us, since we see the same type of disparities in the modern world of commercial cybersecurity.

There is a fundamental reason why cryptography sometimes serves to level the playing field. Cryptography, like pure mathematics, is cerebral — there is no need for large capital investment. To have good cryptography, you don't need to be rich; you only need to be smart. In mathematics, even in the unimaginably difficult conditions of the French and American wars, Vietnam has had a strong tradition (Koblitz 1979, 1990, and 2011), as exemplified by the eminent mathematicians Lê Văn Thiêm, Hoàng Tụy, and the Fields Medalist Ngô Bảo Châu. Given the high value that Vietnamese culture places on pure thought, it is not so surprising that they were able to come up with ciphertext that the NSA could not break.

FIGURE 5. Lê Văn Thiêm (photo on left), Hoàng Tụy (center), and Ngô Bảo Châu (far right).

4. An Unusual Story of Morality among U.S. SIGINT Operators

In a footnote in his book about Nixon and Kissinger (Hersh 1983, pp. 628–629) the American journalist Seymour Hersh tells a remarkable story he learned from interviews with former United States airmen. The story was

again reported (with only a few additional details) in an unredacted part of the declassified NSA history (Hanyok 2002, p. 418).

During the United States Air Force (USAF) "Christmas bombing" of Hanoi in 1972, a large group of intercept operators at two U.S. military intelligence stations — one in Udon, Thailand, and the other in Okinawa, Japan — conducted a "nil heard" protest over a 36-hour period. "Nil heard" is USAF jargon for "I hear nothing," that is, "the intercept operator would claim that he could not hear the transmission of the station he was assigned to copy" (Hanyok 2002, p. 418).

As Hersh explains, from their vantage point in U.S. intelligence the men knew that, after Kissinger's October 1972 statement that "peace is at hand," Hanoi had started demobilizing air defense (the MiG's), and was preparing the city for a big celebration of peace. In those circumstances, the Nixon–Kissinger decision to resume air attacks — presumably in order to terrorize Vietnam into making some last-minute concessions in the peace agreement — infuriated the men. They were so disgusted by the U.S. bombing of civilians that they refused to relay the intercepted communications between the air defense stations and their command. As mentioned before, real-time SIGINT by the USAF was a crucial strategy to reduce Vietnamese success in shooting down American bombers. The action of these men helped the AAA and SAM stations defend Hanoi.

According to Hersh's sources, some time later secret courts-martial of the protesters were conducted in Taiwan (but the USAF to this day declines to confirm this and keeps its information about the incident classified).

The second author recalls his first visit to Vietnam in 1978, just three years after the end of the American war. He and his wife Ann were moved and saddened by an exhibit they saw on Khâm Thiên Street that showed the total destruction of homes in the Christmas bombing. On 26 December 1972, 283 civilians died on that street alone. It was one of many horrible atrocities committed by the USAF.

The protest action by the USAF intercept officers probably prevented the number of people killed in the bombing raids from being even greater than it was. Those SIGINT workers faced a difficult moral choice: help save the USAF pilots from the anti-aircraft artillery and surface-to-air missiles, or help defend the innocent people of Hanoi from the bombs. They chose the second.

There has been a lot of interest in recent years — especially since the Edward Snowden revelations — in moral and ethical issues connected with communications intelligence. Snowden himself is often seen as a rare example of moral courage of someone working "in the belly of the beast." We now know that there are much earlier precedents for people making a bold decision at great personal risk. Almost a half century after the Christmas bombing of Hanoi we should pause to salute the SIGINT operators who showed morality and courage at a moment when brutal atrocities were being committed against innocent people.

FIGURE 6. Khâm Thiên Street soon after the Christmas bombing by the U.S. Air Force. We see what Gen. Curtis LeMay meant by "bomb them back into the Stone Age."

About the authors

Phan Dương Hiệu received his PhD in cryptography from the École Normale Supérieure in 2005. He is currently a professor at the XLIM, Université de Limoges, France. His research focuses on the design of cryptographic schemes. Since 2013, he has been a member of the steering committee of Asiacrypt. He has served on the program committees of several international conferences, including Eurocrypt, Asiacrypt, and PKC.

Neal Koblitz received his PhD in mathematics from Princeton in 1974, and since 1979 he has been at the University of Washington. He is the inventor of hyperelliptic curve cryptography and co-inventor of elliptic curve cryptography. In recent years his research (joint with Alfred Menezes) has focused on critiques of misuses of mathematics in cryptography. Neal and his wife Ann have been collaborating with the Hanoi Mathematical Institute and the Vietnam Women's Union for over thirty years.

Acknowledgments

We wish to thank Thomas Bass, Larry Berman, Christopher Goscha, Trần Kim Phượng, Merle Pribbenow, and Brian Snow for helpful information and

insights, and Ann Hibner Koblitz and Alfred Menezes for editorial assistance. Of course, the opinions expressed and any errors are the responsibility of the authors.

References

[1] Anderson, R. J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Wiley.

[2] Ban Cơ Yếu (Cryptographic Bureau). n.d. *Cơ Yếu Công An Nhân Dân Biên Niên Sự Kiện (1945–1985)* (History of the Cryptographic Section of the People's Police, 1945–1985).

[3] Bass, T. A. 2009. *The Spy Who Loved Us: The Vietnam War and Phạm Xuân Ẩn's Dangerous Game*, Public Affairs.

[4] Berman, L. 2007. *Perfect Spy: The Incredible Double Life of Phạm Xuân Ẩn, Time Magazine Reporter and Vietnamese Communist Agent*, Smithsonian.

[5] Bình, N. T. 2013. *Family, Friends, and Country*, translated by L. Borton, Tri Thức Pub. House.

[6] Borrmann, D. A., W. T. Kvetkas, C. V. Brown, M. J. Flatley, and R. Hunt. 2013. *The History of Traffic Analysis: World War I – Vietnam*, Center for Cryptologic History, National Security Agency.

[7] Centre historique des archives, Service Historique de la Défense, Vincennes, France. "Archives de Indochine: la sous-série GR 10H (1867-1956)," "3ème bureau," "Service du Chiffre" GR 10 H 326 et "Transmission et Chiffre" GR 10 H 3315-3316.

[8] Eisenhower, D. D. 1965. *The White House Years: Waging Peace 1956-1961*, Doubleday and Co.

[9] Goscha, C. 2012. Wiring decolonization: Turning technology against the colonizer during the Indochina War, 1945–1954, *Comparative Studies in Society and History*, 54 (4):798–831.

[10] Hanyok, R. J. 2002. *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975*, National Security Agency, available at http://fas.org/irp/nsa/spartans/

[11] Hersh, S. 1983. *The Price of Power: Kissinger in the Nixon White House*, Summit Books.

[12] Interview with Archimedes L. A. Patti. 1981. http://openvault.wgbh.org/catalog/vietnam-bf3262-interview-with-archimedes-l-a-patti-1981

[13] Johnson, T. R. 1995. *American Cryptology during the Cold War, 1945-1989; Book II: Centralization Wins, 1960-1972*, National Security Agency and Center for Cryptologic History.

[14] Koblitz, N. 1979. A mathematical visit to Hanoi, *The Mathematical Intelligencer*, 2 (1):38-42.

[15] Koblitz, N. 1990. Recollections of mathematics in a country under seige (An interview with Professor Hoàng Tụy), *The Mathematical Intelligencer*, 12 (3):16-34.

[16] Koblitz, N. 2011. Interview with Professor Ngô Bảo Châu, *The Mathematical Intelligencer*, 33 (1):46-50.

[17] Myer, C. R. 1989. Viet Cong SIGINT and U.S. Army COMSEC in Vietnam, *Cryptologia*, 13 (2):143-150.

[18] National Security Agency and Center for Cryptologic History. 2014. *Essential Matters: History of the Cryptographic Branch of the People's Army of Vietnam 1945-1975*, translation of 1990 Vietnamese government publication, available from Amazon Digital Services.

[19] National Security Agency. 2007. Vietnam: A SIGINT paradox (Part I), declassified and approved for release on 27 February 2007, https:

//www.nsa.gov/news-features/declassified-documents/crypto-almanac-50th/assets/files/Vietnam_A_SIGINT_Paradox_Part_I.pdf
[20] Phượng, T. K. 2016. Personal communications with first author, August 2016.
[21] Pribbenow, M. L. 2014. *The Soviet-Vietnamese Intelligence Relationship during the Vietnam War: Cooperation and Conflict*, Woodrow Wilson International Center for Scholars Cold War International History Project Working Paper #73.
[22] Pribbenow, M. L. 2016a. Personal communications with second author, February 2016.
[23] Pribbenow, M. L. 2016b. Email to second author, 1 September 2016.
[24] Snow, B. 2015. Personal communications with second author, October 2015.
[25] Tàu, N. V. (Tư Cang). 2016. Interview by L. Berman, July 2016.

Laboratoire XLIM, Université de Limoges, 123 avenue Albert Thomas 87060, Limoges Cédex, France
E-mail address: duong-hieu.phan@xlim.fr

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195, U.S.A.
E-mail address: koblitz@uw.edu