A. Carlson, S. R. Mikkilineni, M. W. Totaro, R. B. Wells and R. E. Hiromoto. (Jul. 19-22, 2022). Equivalence of Product Ciphers to Substitution Ciphers and their Security Implications, *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, Shenzhen, China, 2022, pp. 1-6, doi: https://doi.org/10.1109/ISNCC55209.2022.9851719]

Equivalence of Product Ciphers to Substitution Ciphers and their Security Implications

Albert Carlson[*], **Sai Ranganath Mikkilineni**[†], **Michael W. Totaro**[‡], **Richard B. Wells**[§], and **Robert E. Hiromoto**[¶].

[*] Computer Science Department, Austin Community College, Austin, TX, USA.

[†] [‡]Intelligent Systems, Modeling and Simulation, (ISMS) Research Lab, Center for Advanced Computer Studies (CACS), University of Louisiana at Lafayette, Lafayette, LA, USA.

[§] Microelectronics Research and Communications Institute, University of Idaho, Moscow, ID, USA.

[¶] Department of Computer Science, University of Idaho, Moscow, ID, USA.

*Email: *albert.carlson@austincc.edu, †sai-ranganath.mikkilineni1@louisiana.edu, ‡michael.totaro@louisiana.edu, §rwells@mrc.uidaho.edu, ¶hiromoto@uidaho.edu.*

***Abstract*—Product/Compound ciphers composed of multi-byte permutations and substitutions are generally considered to be more secure than their stand alone individual component-cipher counterparts (i.e., substitution (S) and permutation (P) ciphers). In this paper, we show that a permutation-substitution-permutation (PSP) cipher that uses any form of regular byte-block boundaries, along with a regular encoding (such as ASCII), is no more secure than a multi-byte S cipher. In addition, we also show that under certain conditions, a PSP cipher can be reduced to an S cipher. In addition to introducing the concept of isomorphic cipher reduction, we show that our theoretical findings translate into practical means by using a plaintext attack. In doing so, we shed light on the problems of encryption security that arise due to employing a product cipher in conjunction with any form of regular byte-block boundaries, and propose appropriate countermeasures.**

***Keywords*—** *encryption, decryption, set theoretic estimation, cipher, block cipher, permutation, cryptography, applications to cryptography, set theory, set theoretic model theory, byte-block boundaries, substitution, cryptanalysis, isomorphic cipher reduction*

I. Background

A. Unicity Distance

In his 1949 work, "Communication Theory of Secrecy Systems" [1], Shannon introduced the concepts of *unicity distance* and *entropy*. The duo together has become an accepted measure of security provided by an encryption system. The unicity distance, n, is defined by Shannon as:

$$n = \frac{log|K_C|}{R_\lambda log|A|} \tag{1}$$

where R_λ is the redundancy of symbols in the language λ and K_C is the keyspace for a cipher C. For any given language, the respective R_λ (overall redundancy) and the alphabet size ($|A|$) are constant; however, the cipher type and its associated keyspace (K) are variable.

978-1-6654-8544-9/22/$31.00 ©2022 IEEE

The unicity distance increases when the keyspace of a cipher is increased. Consider the keyspace for a substitution cipher (S cipher) [2], [3] given by:

$$|K_S| = (|A|!) \tag{2}$$

Thus, to increase the size of the alphabet we group multiple symbols in a text together and encrypt them as a single symbol. We refer to these new grouped symbols together as a "meta-alphabet" comprising of "meta-symbols". The meta-alphabet and meta-symbols collectively define a meta-language [4]. As the name suggests, a meta-language is representative of the language λ. The total number of possible combinations of symbols from an alphabet of size $|A|$ in a block comprised of m characters is $|A|^m$, and the keyspace for the S cipher for a block B of size m is: $K_B = (|A|^m)!$.

Now, let S_S be the security measure used to compare two block-substitution ciphers with block sizes of m and n (where $m > n$), respectively. Then, S_S can be defined in terms of the ratio of their unicity distances (and in turn with their block sizes), as:

$$S_S = \frac{n_{S_m}}{n_{S_n}} = \frac{n}{m}\frac{log(A^m!)}{log(A^n!)} > 1 \tag{3}$$

For $m > n$ and $n \geq 1$, S_S will always increase as m increases. Therefore, the security of an S cipher increases (simultaneously with unicity distance) as the block size increases. Another security as a function of block size is shown in Figure 1.

Besides increasing the block size to increase the keyspace, increasing the total number of times a message is encrypted can also increase the keyspace; this is done using compounding ciphers (also known as product ciphers) discussed by Shannon in [1]. When product ciphers use a good mixing transformation, as discussed by Wells [2] and Stinson [5], the total number of keys for the resulting cipher is obtained by multiplying the keyspace for each cipher involved. Thus, the keyspace for a product cipher with p number of ciphers is given as:

$$|K_{productcipher}| = \prod_{i=1}^{p} K_i \tag{4}$$

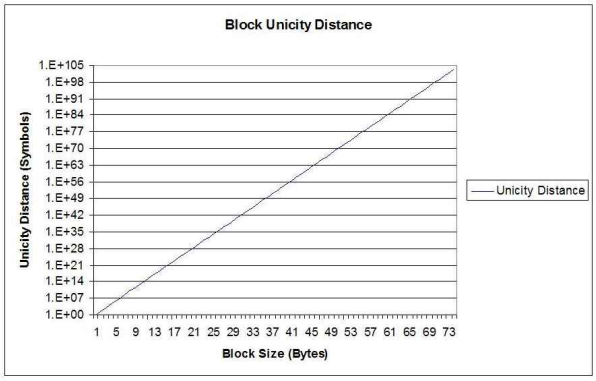

Fig. 1: Unicity Distance for a Substitution Cipher of n-Byte Blocks

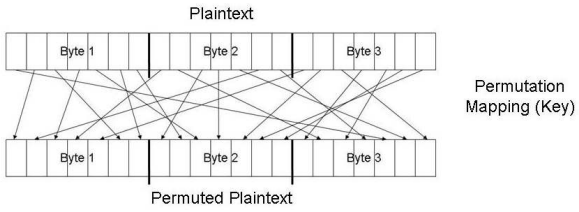

Fig. 2: Permutation Cipher

Since Shannon introduced the concept of increasing security by compounding ciphers in [1], the general consensus is that product ciphers of the form PSP [1], [2], [5] are more secure than a cipher employing their individual standalone counterparts; however, this does not hold true for block ciphers, whose encryption algorithms end at byte (character) boundaries, and are encoded using ASCII. Blocks with an integral character size, suffer from a significant weakness; that is, information is confined within the block. As such, we hypothesize that, as the block size of the PSP cipher increases above 2, the additional security gained is rendered insignificant when compared to a simple substitution cipher of the same block size.

In the following section, we establish the vulnerability of product ciphers by reducing a duplex-product (PS) cipher into an S cipher, followed by the reduction of a triplex-product (PSP) cipher into an S cipher. By doing so, in theory, we establish that the security gain resulting from compounding, is rendered negligible when we increase the complexity of encryption with block sizes of regular intervals. Then, using a plaintext attack, we demonstrate that the previously established theoretical findings translate into practical application. This is then followed by a summary of our conclusions and future work.

II. PS Equivalence to S in Security

Since the block ciphers of PS or PSP type are composed of a P cipher, where a key represents a mapping, and the keyspace for the P cipher [2], [3], [6] is given as:

$$K_P = b! \tag{5}$$

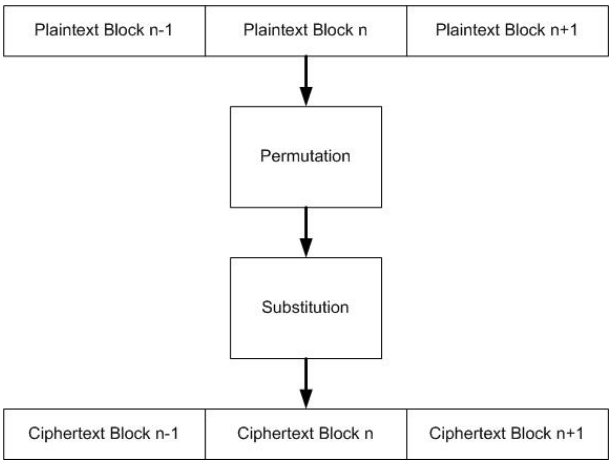

Fig. 3: PS Type Cipher

where, b is the number of bits in the block.

Similarly, since the S cipher maps an alphabet A to another group of symbols A' (i.e., $A \mapsto A'$), it is possible that $A = A'$. As stated previously, substitution cipher(s) can be applied to blocks of letters at a time, instead of one letter at a time; e.g., mapping a two characters block to another two character group. Now, Combining both P and S ciphers into one block cipher using identical block boundaries results in a keyspace of size $b!|A|!$ (based on Eqns. 2, 4, and 5. Extending the block cipher to a PSP cipher, the size of the keyspace is given by $b!|A|!b!$. Although the keyspace increases exponentially with each new cipher added to the product cipher; does this additional overhead involved in the encryption by a PS or a PSP cipher translate into increased security? To address this question, we compare the security of a block substitution cipher to a PS type cipher, and then to a PSP type cipher.

Cipher Reduction: A cipher C_1 using key k_i and encryption given as $E_{k_i,C_1}(M)$ is said to be reduced to cipher C_2 for a message M [7], iff,

$$\forall k_i, M \exists k_j | E_{k_i,C_1}(M) = E_{k_j,C_2}(M). \tag{6}$$

Now, consider a message encrypted by a permutation cipher, followed by a substitution cipher. Without the loss of generality, let the plaintext consist only of lower case alphabetic English characters with all the spaces and punctuation removed [8]. The message uses a standard ASCII encoding and the permutation employs a three character (byte) block. Under the assumption that the encrypted message's byte and block boundaries are known, let's explore the equivalence of a PS cipher to an S cipher through the following theorem:

Theorem 1: *Product ciphers of the form PS or SP aligned at character byte boundaries provide a negligible amount of security (in terms of unicity distance) over a block substitution cipher with the same block size.*

Proof: Let the number of bits in a block be represented by b_m. If the block begins at a byte boundary, then $b_m = m * e$, where m is the number of bytes in a block and e is the number of bits in a byte. While, the number of symbols in the alphabet is given by $|A|$; for a block of m characters with single character/byte, the number of possible combinations of characters in the block is given by $|A|^m$(as in [2], [3]). The

repetition/redundancy in an arbitrary language, λ, is given by R_λ [1].

The product cipher PS is composed of a permutation of b_m bits. For a substitution cipher of m characters with an alphabet A, there are at most of $|A|^m$ possible symbols [2]. Therefore, a PS cipher will have a keyspace of $|K_S| \times |K_P| = b_m!|A|^m!$ (based on Eqns. 2, 4, and 5). This is an upper bound for the keyspace, since some of the possible combinations might be rendered forbidden by the language [9] (i.e. never encountered in the language, such as 'qwz' in English language [10]). Since the uncity distance is regarded as either a lower bound or a mean measure, and from Eqn. 1, the unicity distance for a PS cipher, n_{ps} is given as,

$$n_{ps} \leq \frac{log(b_m!|A|^m!)}{R_\lambda log(|A|^m)},$$

whereas, for an S cipher of the same block size, the unicity distance, n_s is,

$$n_s \leq \frac{log(|A|^m!)}{R_\lambda log(|A|^m)}.$$

Based on Eqn. 3, let

$$S_R = \frac{n_{ps}}{n_s}$$

be a measure of the relative security of the two ciphers. Then,

$$S_R \quad = \quad \frac{log(|A|^m!) + log(b_m!)}{log(|A|^m!)}$$

Therefore,

$$S_R = 1 + \frac{log(b_m!)}{log(|A|^m!)} \tag{7}$$

Since, we use Set Theoretic Estimation (STE) [11] [12] [13], and set methodology for our analysis in which the second term of Eqn. 7 is analogous to the bounded error term. Therefore, let

$$\epsilon = \frac{log(b_m!)}{log(|A|^m!)}. \tag{8}$$

Then,

$$S_R = 1 + \epsilon.$$

Since the minimum number of bits in a representation is determined by the application of Hartley's Equation [14]. The lower bound for b_m can be defined as:

$$b_m = \lceil log_2 |A|^m \rceil. \tag{9}$$

Substituting the lower bound of the representation into Eqn. 8, results in

$$\epsilon = \frac{log(\lceil (log_2|A|^m) \rceil !)}{log(|A|^m!)} < 1$$

Since, $\forall x > 1$; $log_2(x) < x$. Therefore, $\epsilon < 1$; and ϵ decreases as m increases.

m	$log(b_m!)$	$log(A^m!)$	ϵ
1	4.605	26.6056	0.173103
2	13.3206	1621.275	0.008216
3	23.7927	66978.08	0.000355
4	35.4202	2.40×10^6	1.49×10^{-5}
5	47.91165	7.89×10^7	6.07×10^{-7}
6	61.09391	2.49×10^9	2.46×10^{-8}
7	74.85147	7.61×10^{10}	9.84×10^{-10}
8	89.10342	2.27×10^{12}	3.92×10^{-11}
9	103.787	6.68×10^{13}	1.55×10^{-12}
10	118.8547	1.93×10^{15}	6.14×10^{-14}

TABLE I: Security for a Block of m Bytes

Expansion algorithms (such as, DES [3]) are commonly used in encryption to fill a block with permuted bits and extra bits derived from the input data. The mapping of an expansion algorithm is $b_m \mapsto b_{m'}$ bits, where, $b_{m'} = b_m + n$. The expansion to $b_{m'}$ must be unique because $b_m \mapsto b'_m$ is both one-to-one and onto mapping. Therefore, the number of characters that can be represented by $b_{m'}$ is $2^{b_{m'}}$; thus,

$$\forall b_{m'} > 0 \rightarrow b_{m'} < 2^{b_{m'}}$$

and,

$$\forall b_{m'} > 0 \rightarrow log(b_{m'}) < log(2^{b_{m'}}).$$

So, the expansion of the symbol merely maps the alphabetic character to a different symbol representation. Therefore, there is no significant security-advantage gained by expanding the size of the character representation [15]. □

Corollary I: *The relative security for a PSP cipher is given by* $S = 1 + 2\epsilon$

Proof: Same as Theorem 1, but, with the keyspace for a PSP cipher given by $b_m!|A|^m!b_m!$ instead of PS cipher's $b_m!|A|^m!$ □

A. Supplementary Material for Theorem 1

Values of ϵ (see Equation 8) using ASCII encoding for small block sizes are shown in Table-I, and Figure-5. While Figure-4 illustrates the behavior of S_R as a function of block size; specifically for blocks of size $m > 3$; we can see from Figure 4 that the relative security S_R between PS and S ciphers is indeed negligible.

S_R from Figure-4 represents an upper bound on the difference between a PS or SP cipher and an S cipher. For blocks of size $m \leq 3$ there is a small but, relatively notable difference in the respective unicity distances of the PS and S ciphers predicted using the unicity distance Eqn. 7. No difference would exist if the PS and S ciphers were the same cipher. In fact, the PS cipher is a type of S cipher if the S cipher maps from a symbol of size $|Block|$, and both ciphers employ the same block boundaries.

III. PSP Equivalence to S

In conjunction with Eqn. (6):

Axiom 1: In order for cipher a C_1 to be reduced to cipher C_2, the range of the encryption function for C_1 must be a subset of the range of the encryption function for C_2. That is,

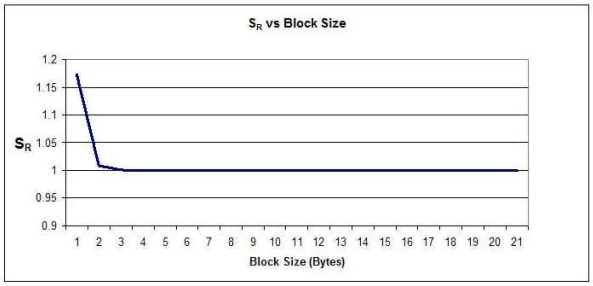

Fig. 4: S_R vs. Block Size (in bytes)

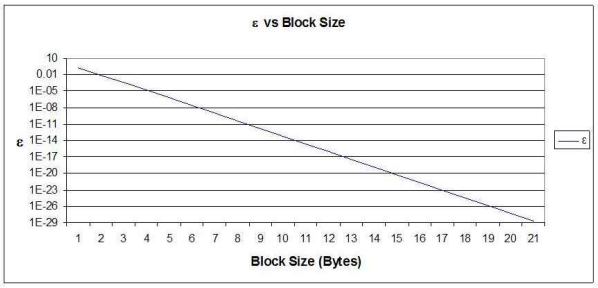

Fig. 5: ϵ vs. Block Size (in bytes)

$$\forall M; E_{k_i,C_1}(M) \in E_{k_j,C_2}(M)$$

Axiom 2: Any cipher C_1 shall reduce to itself, when, $k_i = k_j$.

Axiom 3: If cipher C_1 reduces to a cipher C_2, then cipher C_1 can be replaced by cipher C_2 by using the appropriate key for C_2.

Theorem 2: *A permutation cipher $P(E_k(M))$ reduces to a substitution cipher S within the encoded representation of a symbol.*

Proof: Let the symbol s_i from an alphabet A be represented by a collection of n bits, where $n = \lceil log_2(|A|) \rceil$ [14]. Let B be the set of all possible values represented by various combinations of the collection of n bits, and the values in set B range from 0 to $2^n - 1$; therefore, $A \subseteq B$. Since a permutation cipher [3] preserves the total number of respective '1' and '0' bits, but rearranges them into another symbol by preserving the total number of bits, $E_k(A) \in B$ (i.e., a permutation results in a mapping of $A \mapsto B$), therefore, under above stated conditions, a permutation cipher is a special case of the substitution cipher. Thus, since a unique substitution key exists for every permutation mapping, $A \mapsto B$ [3], P reduces to S within the boundaries of an encoded symbol. □

The property set for P cipher reduction to the S cipher is composed of mappings from plain text to cipher text where the number of '1' and '0' bits are unchanged in the symbol representations. In general, an n bit block can be extended to an m bit block cipher, where $m \geq n$ and if the extra bits in the expanded m bit representation are ignored. For instance, let n bits of data be mapped to m bits with $n < m$. The extra $m - n$ bits may be an expansion, with some of the n bits being mapped into more than one bit position (such as occurs in many Fiestel round ciphers, like DES [3]). Any key which is identical in the unique mapping of the m bits can be considered the correct key with the remaining duplicate keys ignored while decrypting the message. If the excess $m-n$ keys are randomly generated, those excess bits may also be ignored in the reduction process. However, using randomly generated bits to fill an expanded permutation would be an example of inserting cryptonulls [3] to introduce further difficulty for cryptanalysts.

Lemma: *A substitution cipher does not necessarily reduce to a permutation cipher.*

Proof: Consider that P preserves the total number of respective '1' and '0' bits, but, S may not; we present a **proof by contradiction:** Assume that, S reduces to P in all cases(as opposed to the Proof of Theorem 2). Let the S cipher contain a mapping in which a symbol from $A \mapsto B$ and $|A| = |B|$, but, the total number of bits having the '1' value is even in A and odd in B. Now, as if the P ciphers can only map to encrypted symbols having a constant number of respective bits(i.e., the total number of 1's and 0's need to be the same in both A and B, for a given instance of mapping); therefore, $B \notin P_k(A)$. By contrapositive, in general S does not reduce to P.

Corollary 1: *If cipher C_1 reduces to cipher C_2 it does not necessarily follow that C_2 reduces to C_1.*

Proof: Based on the preceding lemma: P reduces to S but S does not reduce to P. □

Definition: A compound symbol[16], X, is an ordered n-tuple of characters (block) $< x_0, x_1, ..., x_i >$ regarded as comprising a single symbol, where $x_i \in A_\lambda$ and A_λ is the alphabet of language λ.

Corollary 2: *Under the condition of symbol - byte boundary alignment, a PSP cipher is idempotent to an S cipher with identical block boundaries.*

Proof: Let the symbol in a block cipher be a compound symbol [2] defined as being the same size and having the same boundaries as the cipher block. Further, let the S cipher be applied to the same compound symbol. By Theorem 2, P and S ciphers are equivalent within a symbol boundary. Therefore, PSP reduces to $S_0S_1S_2$. Since, S ciphers are idempotent [2] and associative with each other, the $S_0S_1S_2$ cipher reduces to a single S cipher. □

IV. Chosen Plaintext Attack

In this section, we illustrate the equivalence of the SP and S ciphers using a plaintext attack.

A. Experimental Setup:

Assume that the block cipher boundaries and the block size are known, and the alignment condition is met. Without loss of generality, the block size is set to 3 bytes. Now, the plaintext is encrypted by SP, and then the resultant ciphertext is attacked using S.

We treat an entire block as a single character from a meta-language. Thus, each symbol is analyzed to generate common language statistics based on their appearance in English. Language statistics constitute property sets that can be exploited using STE and set methodology ([9], [11]). One group of property sets consisting of m-grams are introduced by Shannon in [1]. The m-grams used in our STE approach, are drawn from a survey of English prose styles from 1600 - 2000 AD [9], and curated from Project Gutenburg [17]. Let each symbol in this meta-language represent an m-gram of English; this

No. 3-grams	% Plaintext Covered
117	25.101%
449	50.025%
1242	75.008%
11315	100.000%

TABLE II: 3-gram Coverage for Attack

% Coverage	Average	Standard Deviation
25%	25.34%	3.66%
50%	50.19%	4.84%
75%	74.78%	5.20%

TABLE III: Chosen Plaintext Results

assumption reduces the total number of symbols in the meta-language's alphabet to the number of unique m-grams allowed in English, and all encryption occurs within a single meta-symbol.

Messages consisting of English language text are represented using ASCII encodings[18]. All non-alphabetic characters are removed from the text to avoid giving clues about words, sentence structure, or punctuation ([3] [8]). The key is assumed to be constant from one block to the next. We then append a small number of known plaintext characters at the start of each message(i.e., expansion). The chosen plaintext consists of a set of m-grams represented as g, where $m = |Block|$, and whose combined probability of the m-gram appearing in English is greater than some known probability x,

$$x = \sum_{i=1}^{n} p(g_i) \tag{10}$$

We define the target coverage as the value of x (see Eqn. 10) resulting from a set of m-grams. The set is applied to an input file and the number of m-grams found in the coverage set, g_{found}, divided by the number of m-grams in the input file, g_{file}, is the "percentage of coverage" for the given m-gram set and input file, and is given by,

$$\text{percent of coverage} = \frac{g_{found}}{g_{file}} \times 100. \tag{11}$$

Even though, each message differs because of the content and the author, x should be close to the calculated percent of coverage for the message.

Since we intend to demonstrate the equivalence of the SP cipher to an S cipher, we are going to select $m-$grams with high frequency of occurrence in the target language (here, English) and then encrypt using an SP cipher, and then we decrypt it using an S cipher. This equivalence was anticipated by Lucks [19], who showed that a disproportionate amount of a message is represented by a very small number of language blocks(here, $m-$grams).

B. Tests and Results:

The chosen plaintext is selected from the 3-grams set, with the highest frequency of occurrence in our m-gram property set. The mapping for the substitution is recovered by selecting the 3-grams seen most frequently in our corpus, and applying them to the encryption process. A table is constructed by matching the known plaintext to the output of the encryption applied to the known plaintext. The table comprises a partial key for S cipher that is used to decrypt the SP encrypted message. The number of correctly decrypted blocks, and the coverage are calculated. Table II shows the number of 3-grams required to recover portions of the plaintext. For example, 449 3-grams are required to recover an average of 50% of the plaintext.

Each of the test files is run using the chosen plaintext attack with m-grams, providing a 25%, 50%, and 75% respective coverage of a typical English language text. The files are used in a total of 813,363 tests, and the results are summarized in Table III. Since an S cipher preserves language statistics ([2], [3]), including symbol frequency; we expected that the amount of correctly decrypted data using the chosen plaintext attack would closely approximate to the coverage statistically represented by the selected set.

Unlike the above case, the same plaintext symbol can map to more than one ciphertext symbol, when ciphers do not preserve a unique mapping of $A \mapsto A'$ resulting in a different symbol frequency.

In our tests, frequency varied from the calculated coverage (based on Eqn. 11) by a high of 1.36% to a low of 0.012% from the predicted coverage; this deviation from the average was expected due to the semiotic [20] differences between the authors of the literature used in our tests. As a control, several files containing non-English text (such as Norwegian, Latin, Spanish, Italian, Welsh, and Polish) were used. The number of decrypted 3-grams for each non-English text is between 4% and 15% of the total text, and are easy to distinguish from the English texts. As the coverage of the English files increases, the presence of the non-English files gives rise to a larger standard deviation, as reported in [16]. The results indicate that the chosen plaintext attack was successful for an S cipher. Thus, ciphers of the form SP and PSP act like an S ciphers, as demonstrated by an approximately 99% correct decryption using this attack against English language texts.

V. Summary, Conclusion, and Future Work

The practice of strengthening ciphers using the S cipher in tandem with P and linear ciphers is not always as strong as presumed. We have shown that SP product ciphers aligned at byte boundaries are negligibly more secure than an S block cipher of the same block size. While Shannon claimed that a good mix of ciphers increases security, we have shown that SP ciphers can offer no increase in the unicity distance as compared to S ciphers, thus, no notable improvement in security.

We also introduced and illustrated the concept of cipher reduction, allowing one type of cipher to be replaced by another type of cipher under certain conditions. Reducing a cipher can occur when the cipher replacing the original cipher can encrypt all messages identically to the cipher it replaces. To substantiate this, we have shown that the P cipher reduces to the S cipher if the size of both symbols is identical. In conjunction to that, while cipher C_1 might reduce to C_2, the vice versa is not guaranteed. To support this, We showed that while P reduces to S for an identical symbol size, S does not reduce to P. Using reduction and idempotence, we further demonstrated that the PSP cipher is equivalent to the S cipher if the block size is identical and the alignment condition is met.

Based on the results of reducing an SP cipher to an S cipher, we illustrated a chosen plaintext attack on the SP cipher. Employing an STE approach that utilizes the property set of symbol frequency in the English language, we selected a set of high frequency m-grams in English. The m-grams in the set are appended to the front of the message and as they are encrypted, the m-grams are recorded along with the associated encryption. The percentage of message decrypted closely matches the statistical frequency of the chosen m-gram set. Thus, we have demonstrated the effects of plaintext coverage in the decryption of an SP cipher. The cases of a PS and PSP cipher can be expected to yield the same results as the SP cipher under Corollary 2.

In conclusion, ciphers employing combinations of permutation and substitution must not employ regular sized blocks that have byte boundaries; such ciphers make the user susceptible to the same attacks as the S cipher. As a solution to this security problem, one can employ any of the following strategies: block ciphers that do not use an integral or cyclic block boundaries; encryption that diffuses across byte boundaries; avoidance of byte boundaries altogether; and the use of large block size for encryption.

In our future work, we plan to address the issues of confusion and diffusion using Cipher Block Chaining (CBC) [3].

REFERENCES

[1] Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656 – 715, 1949.

[2] Richard Wells. *Applied Coding and Information Theory*. Prentice Hall, Upper Saddle River, 1999.

[3] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons Inc., New York, 2nd edition, 1996.

[4] A van Wijngaarden, BJ Mailloux, JEL Peck, CHA Koster, M Sintzoff, CH Lindsey, LGLT Meertens, and RG Fisker. Language and metalanguage. In *Revised Report on the Algorithmic Language Algol 68*, pages 17–35. Springer, 1976.

[5] Douglas R. Stinson. *Cryptography, Theory and Practice*. Chapman & Hall/CRC, Boca Raton, 3rd edition, 2006.

[6] Statistics http://usa.kaspersky.com/. Internet, 2007.

[7] Bhaskar Ghosh, Indira Dutta, Shivanjali Khare, Albert Carlson, and Michael Totaro. Isomorphic cipher reduction. 2021.

[8] Timothy J. Shimeall and Jonathan M. Spring. Chapter 8 - resistance strategies: Symmetric encryption. In Timothy J. Shimeall and Jonathan M. Spring, editors, *Introduction to Information Security*, pages 155–186. Syngress, Boston, 2014.

[9] Albert Carlson and Robert Hiromoto. Using set theoretic estimation to implement shannon secrecy theory. In *The Proceedings of the Third IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pages 435 – 438, 2005.

[10] Robert Lewand. *Cryptological Mathematics*. Mathematical Association of America, Washington D.C., 2000.

[11] Patrick Combettes. The foundations of set theoretic estimation. *Proceedings of the IEEE*, 81(2):182 – 208, 1993.

[12] Hans Witsenhausen. Sets of possible states of linear systems given perturbed observation. *IEEE Transactions on Automatic Control*, AC-13(1):556 – 558, 1968.

[13] Fred Schweppe. Recursive state estimation: Unknown but bounded errors and system inputs. *IEEE Transactions on Automatic Control*, AC-13(1):22 – 28, 1968.

[14] Paul Garrett. *The Mathematics of Coding Theory*. Pearson/Prentice Hall, Upper Saddle River, 2004.

[15] Thomas Cover and Joy Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc, New York, 2nd edition, 2005.

[16] Albert Carlson. *Set Theoretic Estimation Applied to the Information Content of Ciphers and Decryption*. PhD thesis, University of Idaho, 2012.

[17] The Gutenburg Project. Main page-http://www.gutenburg.net. Internet, 2008.

[18] Robert W. Shirey. Internet Security Glossary, Version 2. RFC 4949, August 2007.

[19] M. Lucks. A constraint satisfaction algorithm for the automated decryption of simple substitution ciphers. In *CRYPTO 1988*. CRYPTO, 1988.

[20] Daniel Chandler. *Semiotics for beginners*. Routledge, Milton Park, UK., 1994.