COMP-547  Winter 2017
Cryptography and Data Security

Claude Crépeau
McGill University
<table>
<thead>
<tr>
<th>Tasks</th>
<th>Encryption</th>
<th>Authentication</th>
<th>Identification</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symmetric Informational</strong></td>
<td>Miller–Vernam One-Time PAD</td>
<td>Wegman–Carter Universal Hash</td>
<td>Simple Solutions</td>
<td>Quantum Key Distribution</td>
</tr>
<tr>
<td><strong>Symmetric Computational</strong></td>
<td>from PRBG from PRFG DES, AES, etc</td>
<td>from PRBG from PRFG DES, AES, etc</td>
<td>from PRBG from PRFG DES, AES, etc</td>
<td>Quantum Attacks, Q-Safety</td>
</tr>
<tr>
<td><strong>Asymmetric Computational</strong></td>
<td>RSA, ElGamal, Blum-Goldwasser</td>
<td>RSA, DSA, etc</td>
<td>Guilloux-Quisquater, Schnor, etc</td>
<td>Quantum Attacks, Q-Safety</td>
</tr>
</tbody>
</table>

**Status**
- **DONE**
- **IN PROGRESS**
- **TO DO**
- **GIVE UP**
<table>
<thead>
<tr>
<th>Time</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>Tue</td>
<td>Thu</td>
<td>Fri</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30</td>
<td>Mon</td>
<td>Tue</td>
<td>Wed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td>Mon</td>
<td>Tue</td>
<td>Wed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:30</td>
<td>Mon</td>
<td>Tue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td>Mon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td>Mon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:00</td>
<td>Mon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Office Hours:**
- Claude: TR-2110
- Krtin: MC-TBA
- comp610: MC-103

**Note:**
- MC = MCENG = McConnell
- TR = ENGTR = Trottier
Classical Cryptography
Information

Theoretical

Cryptography
Information Theoretical Cryptography

- Key Distribution
- Encryption
- Authentication
- Identification
Will you marry me?

Divorce your wife first!

The papers are in the mail...

OK, I will!
Key Distribution
Encryption
Will you marry me?

8RdewtU5qkLa$es!T9@

Decryption

Encryption

8RdewtU5qkLa$es!T9@

Will you marry me?
Encryption

8Rdewtu5qkLa$esIT9@

Decryption

l(D%eXhDqliykl#2cv7dEwnMs

Divorce your wife first!
Symmetric Encryption

Encryption

Decryption

Information Theoretical Security
Symmetric Encryption

Ceasar’s Cipher
MILLER-VERNAM Cipher
MILLER-VERNAM Cipher

$m \oplus k = c$

$\begin{array}{ccc}
1 & 1 & 0 \\
0 & 1 & 1 \\
1 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
0 & 0 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 0 & 1 \\
0 & 1 & 1 \\
0 & 1 & 1 \\
1 & 1 & 0 \\
\end{array}$

$\oplus =$

$\begin{array}{ccc}
0 & 1 & 1 \\
1 & 1 & 0 \\
0 & 1 & 1 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 1 & 0 \\
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 1 & 0 \\
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0 \\
0 & 1 & 1 \\
\end{array}$

$c \oplus k = m$
Miller-Vernam One-Time Pad

\[ m_1 \oplus k = c_1 \]
\[ m_2 \oplus k = c_2 \]

\[ c_1 \oplus c_2 = m_1 \oplus m_2 \]
\[ M_0 \oplus C_0 = M_1 \oplus C_1 = X \]
Authentication
Authentication

Will you marry me?

Verification

Valid

marrу me?

Authentication

Will you marry me?
Authentication

Will you marry me?

Divorce your wife first!

The papers are in the mail...

OK, I will!
Symmetric Authentication

(m, t)

Authentication
\[ t := A_k(m) \]

Verification
\[ t = A_k(m) \]
Will you marry me?

Verification

Authentication

INVALID  marry me?

Will you marry me?
Will you marry me?

No, I never will!
Symmetric Authentication

M          K          T

Authentication

Verification

Information Theoretical Security
Information Theoretical Security

**Impersonation**

\[(m, t)\]

**Substitution**

\[(m, t) \rightarrow (m', t')\]
Wegman-Carter
One-Time Authentication

message ⊕ key = tag

message ⊕ key = tag
Wegman-Carter
One-Time Authentication

message \oplus \text{key} = \text{tag}

message \oplus \text{key} = \text{tag}
identification
One-Time Identification

ALICE

OK

Key exchange between ALICE and OK.
Des fraudeurs déjouent la sécurité des cartes de débit

( Crooks bypass ATM Security )

Québec et qui pourrait compromettre sérieusement l'utilisation des cartes de débit bancaires.

Les fraudeurs, une dizaine au total, ont été commises jeudi de la semaine dernière, entre 18 h et 21 h, à l'intérieur du dépanneur Couche-Tard, du 670, boulevard Laurier, à Mont-Saint-Hilaire.

Les victimes sont des clients de ce commerce qui ont payé leur achat avec leur carte de débit automatique, sans savoir que le lecteur (skimmer) utilisé avait été trafiqué par les fraudeurs et installé dans le commerce avec la complicité du commis.

Pour payer leur achat, les clients ont présenté leur carte de débit et composé leur NIP, avant que le commis ne leur remette, comme si tout était normal, le petit reçu indiquant le montant de la transaction et indiquant que celle-ci avait été approuvée par l'institution bancaire.

Ce que les clients ne savaient pas, et qu'ils ne savaient probablement toujours pas, c'est que le lecteur n'était pas branché au système Interac. Ils ne pouvaient pas imaginer non plus que l'appareil avait été trafiqué de façon à permettre aux fraudeurs d'enregistrer leur numéro de compte et leur numéro d'identification personnel (NIP).

JEUNE NOIR RECHERCHÉ

Les informations détectées par les policiers, qui s'apprêtent à déposer des accusations de fraude contre le commis du dépanneur, indiquent qu'un homme d'une vingtaine d'années, de race noire, faisant environ 5 pieds, huit pouces et 165 livres, se serait présenté au dépanneur du boulevard Laurier vers 18 h, le 8 mars, pour conclure un marché avec l'employé du commerce.

Il aurait offert 10 000 $ à ce dernier pour braquer durant la soirée son «skimmer» trafiqué. L'employé aurait accepté et reçu sur-le-champ quelques centaines de dollars pour régler comptant les transactions.

Selon le commis, qui a été interrogé par le sergent-détective Dery, une dizaine de transactions seulement ont été effectuées avec le lecteur trafiqué. Et jusqu'à preuve du contraire, les comptes bancaires des clients, qui ne sont toujours pas identifiés, n'ont pas été vidés par les fraudeurs.

Arrêté par les policiers, le commis a expliqué qu'il n'a jamais touché les 10 000 $ promis. Les fraudeurs ne lui auraient remis que 400 $ pour ce service.

Tous les clients qui ont fréquenté le dépanneur Couche-Tard entre 18 h et 21 h le 8 mars sont invités à communiquer avec M. Dery au 467-3371.

Les policiers sont par ailleurs à la recherche du jeune homme de race noire d'une vingtaine d'années qui se déplace en compagnie de deux complices d'origine libanaise.
Impersonation

ALICE → OK → ALICE

ALICE → OK → ALICE
**Impersonation**

1. Alice shares an encryption key.
2. Alice verifies the key is correct.
3. Alice impersonates another party.
4. Alice is impersonated by another party.

The process involves key exchange and verification steps to establish trust and prevent unauthorized access.
Impersonation

ALICE

OK

ALICE

OK

ALICE

OK

ALICE

OK

ALICE

OK

ALICE

OK

ALICE

OK
One-Time Identification

ALICE

OK

ALICE

OK
Quantum Cryptography
Information Theoretical Cryptography

Quantum key distribution
Ambiguous Coding Scheme

0

1

+ [Graph]

× [Graph]
Calcite Crystal & Photodetection
Quantum Key Distribution
Quantum Key Distribution

<table>
<thead>
<tr>
<th></th>
<th>A: 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0</th>
<th>B: x x + + x + + + x + + x x x + x x x + + + + x + + + x +</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0 0 1 0 0 1 0 0 1 0 0 0 0 1 1 1 0 0 0 1 1 0 0 0</td>
</tr>
<tr>
<td></td>
<td>A: x + x + + + + x x x x + + + + x x x + + + + x + + + x +</td>
<td>B: 0 0 0 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B: 0 0 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A: 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>A: 0 1 0 1 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 0</td>
<td>B: = = = = ≠ = =</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B: 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A: 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>

Bennett-Brassard
Quantum Key Distribution

- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller very secret classical key
Mandatory Material

- Class notes (course web page)

**INTRODUCTION TO MODERN CRYPTOGRAPHY**
Second Edition
Jonathan Katz
Yehuda Lindell
Evaluation

- 5 homework assignments
- FINAL EXAM : 50%
CIAO !
TELEGRAPHIC CODE

TO INSURE

PRIVACY AND SECRECY

IN THE

TRANSMISSION OF TELEGRAMS.

BY

FRANK MILLER.

NEW YORK:

CHARLES M. CORNEWELL,

247 PEARL STREET.

Copyright 1868, by FRANK MILLER, of Sacramento, California.
Fox inland telegraphing, simplicity and speed are more important than economy. With cablegrams the reverse is the case. Cable codes are mainly composed of vast numbers of phrases, and are so intricate that few country bankers will use them.

Sixteen years' banking experience gives the compiler confidence to hope that this Code will be carefully examined by bankers, and that it will correct a positive evil, to wit, the relying upon hastily formed cryptographs, which continually repeat, and which are therefore dangerous, because, if an operator should decipher such a system, and send a message in such a cipher, great suspicion would arise against all parties having access to such cryptographs.

Any system which allows a cipher word to be used twice with the same significance is open to detection. A little talk with a telegraphic operator will convince one of this fact.

Colonel Myers says: "If signals are to be displayed in the presence of an enemy they must be guarded by ciphers which must be capable of frequent changes, and the rules by which these changes are made must be simple."

The selection of words in this book has been carefully made, assistance being had from experts upon the phrases and cipher words. Names of principal cities, surnames, and Christian names will be found in abundance.

This book contains 12300 words and phrases, each having its cipher-word duly numbered; then follow 1700 cipher-words, the last number thereto being 14000.

A supplementary code, which can be used with this, can thus be made by taking all, or part, of the "extra cipher-words," and forming phrases opposite each to suit any special business.

For the convenience of the majority of users, ten lists are provided with 73 cipher-words to each, for the registering of special phrases.

This system is absolutely secret; it is also simple and quickly operated, as will be proved by a little practice.

It can be used for long messages and for years, care being taken by correspondents to keep each other well supplied with "shift-numbers."

The sender of a message should send by mail an exact translation, for, after some interval of time and loss of "shift-numbers," it will be impossible to again translate the message.

The lists of "shift-numbers" should be kept by one person in each bank, and from him one or more of the "shift-numbers" may be obtained by such clerks as receive or send telegrams.

The sender and receiver must each cancel "shift-numbers" as fast as they are used.

If the sender finds that the addition of a key produces a sum greater than the highest "serial number" (14000) in this book, he must deduct said last "serial number" from said sum and count the excess from the first page.

On the other hand, if the receiver finds that the "serial number" of a cipher-word is less than the key which is to unlock it, he must temporarily add to said "serial number" the highest number in this book and deduct the key from the sum.

This Code in itself does not give any person the right to presume that its use in "plain cipher" has such binding effect as if used in "shifted cipher."

It is evident that many dispatches need not be in cipher, such as ordering money by express from a reserve agent to go to the sender of the telegram, remarks about missing letters, and many others.

Such messages can be put in what we will call "plain cipher," which is taking the "cipher-word" on the same line as printed. But few copies of this code will be in any town, and a message in "plain cipher" would practically insure privacy.

The rule would seem to be that all messages which could be sent verbally by a messenger may be sent in plain English or "plain cipher."

The payment of money, or any other action which would require written authority, and which would not be done when such order was sent verbally by messenger, it is evident, requires a test of genuineness that must be infallible.

Such tests of genuineness and also methods for rendering a message absolutely secret are to be had by the use of "shift-numbers," as hereafter described.

Words should be written plainly, so the operator may not err in sending messages.

Mistakes in sending will sometimes occur: thus C--- and S--- will be confused, making "came" read "same," &c., &c.

Also O- --- and E- E- making "son" read "seen," &c.

Also R-- and S--- making "sail" read "rail," &c.

Also by missing a dot, P will be taken for H; F for A or N; O for E, &c.

HORSE ALPHABET.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A copy of this Code has been sent to each bank in New York City, whose address and "cipher-word" follows hereafter.

A copy has likewise been sent to each bank which is a member (in 1833) of the Clearing House in Chicago, St. Louis, New Orleans, and San Francisco.

This Code is stereotyped and no changes will be made at any time.

**SHIFT-NUMBERS.**

A banker in the West should prepare a list of irregular numbers, to be called "shift-numbers," such as 483, 281, 175, 892, &c.

The differences between such numbers **must not be regular.**

When a shift-number has been applied, or used, it must be erased from the list and not used again.

A copy of the list is to be sent to the New York Banker, who prepares a **different list** and sends copy thereof to the Western Banker.

Each party should enter his own list in black ink in a book, and copy his correspondent's list in red ink upon the opposite page; thus the black figures will denote his "sending numbers," and the red figures will denote his "receiving numbers."

Having occasion to telegraph an order requiring the payment of money, and knowing that an English dispatch would receive no attention, the Western banker will write his dispatch on a sheet of paper, leaving a few lines blank between the written lines.

He will then find his first word in this Code, and copy upon the sheet of paper its number, placing the number under the word.

Under said number (which we will call the "serial-number") he will place the first "shift-number" (say 483). He will then add the two numbers and find their sum, which he will write down.

Underneath this new sum, or number, he will write the "cipher-word" which he shall find in the Code standing alongside of said sum.

Thus he gets the first cipher-word for his telegram.

To the appropriate "serial-number" of the second word he will add the second "shift-number" (say 281), and, finding their sum, he will take the cipher-word which is found opposite said sum.

He will follow the same plan with the remaining words.

---

**EXAMPLE.**

<table>
<thead>
<tr>
<th>Gentleness</th>
<th>Glared</th>
<th>Allegro</th>
<th>Fantasia</th>
</tr>
</thead>
<tbody>
<tr>
<td>5184</td>
<td>5223</td>
<td>401</td>
<td>4163</td>
</tr>
<tr>
<td>488</td>
<td>281</td>
<td>175</td>
<td>892</td>
</tr>
</tbody>
</table>

For many telegrams it will suffice that the common English words be used with a "test word" that shall indicate that the dispatch was genuine as sent. Economy and much safety can also be secured by using a "test word" and placing the rest of the message in "plain cipher"—that is, using the Code as printed without any "shifting."

The sender will, in such cases, take the two right-hand figures of his first "shift-number," and use the test word indicated by such two figures; thus he will use the test word "Abstruse" if his first key is 483, and place the rest of the message in English or in "plain cipher."

The receiver will note that a "test word" is used, and that its number is the same as the two right-hand figures of the key (or "shift-number"), which is then available.

Said "shift-number" must, of course, be then erased by both sender and receiver, for it is void for further use.

**EXAMPLE.**

<table>
<thead>
<tr>
<th>Abstruse</th>
<th>Foredated</th>
<th>Furuncle</th>
<th>Admirers</th>
<th>Disgusted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abstruse</td>
<td>Extended</td>
<td>for eight</td>
<td>days</td>
<td></td>
</tr>
</tbody>
</table>