CIPHER Documentation / Documentation CIPHER

Release 0.1.0

CIPHER Contributors / Contributeurs CIPHER

Nov 28, 2024

NAVIGATION

Canadian Index of Practical Ham Encryption Resources / Index Canadien des Ressources de Chiffrement pour Radioamateur

CHAPTER

ONE

ABOUT / À PROPOS

Welcome to CIPHER (Canadian Index of Practical Ham Encryption Resources), an open-source, community-maintained documentation suite for encryption protocols used in Canadian amateur radio communications.

Bienvenue au CIPHER (Index Canadien des Ressources de Chiffrement pour Radioamateur), une suite de documentation open-source, maintenue par la communauté, pour les protocoles de chiffrement utilisés dans les communications radio amateur canadiennes.

CHAPTER

TWO

PURPOSE

This repository documents encryption protocols for amateur radio, compliant with Canadian regulations which permit encrypted communications provided the protocol and keys are publicly documented. As per Radio Amateurs of Canada, who maintain a public registry of encryption keys, any operator may use encryption as long as the method remains transparent and documented.

Ce dépôt documente les protocoles de chiffrement pour la radio amateur, conformes aux règlements canadiens qui permettent les communications chiffrées à condition que le protocole et les clés soient documentés publiquement. Selon Radio Amateurs du Canada, qui maintient un registre public des clés de chiffrement, tout opérateur peut utiliser le chiffrement tant que la méthode reste transparente et documentée.

- Complete Documentation / Documentation Complète (PDF)

2.1 Contributing Guidelines / Directives de Contribution

2.1.1 English

Version française

2.1.2 How to Contribute

We welcome contributions to CIPHER! Here's how you can help:

1. Fork the repository
2. Create a new branch
3. Add your protocol documentation
4. Submit a pull request

2.1.3 Documentation Standards

Protocol Structure

- 5-character alphanumeric protocol ID (generate using: `python3 -c "import random, string; print(''.join(random.choices(string.ascii_uppercase + string.digits, k=5)))"`)
- Bilingual content (English and French)
- Cross-references between language versions

- Follow RST formatting standards:
  - Sphinx RST Primer
  - RST Documentation

Required Sections

1. Overview:
   - Purpose and basic description
   - Links to relevant tools/references
   - Protocol flexibility statement
2. Standard Operating Procedure:
   - Initialization
   - Transmission Format
   - Example Transmission
3. Implementation Details:
   - Core procedure
   - Examples with test data
   - Look-up tables if needed
4. Security Considerations:
   - Security limitations
   - Intended use cases

2.1.4 Testing

Before submitting:

1. Build documentation locally:

   Install dependencies: `poetry install`

   Build docs: `cd docs && poetry run make html`
2. Verify both language versions:
   - Check cross-references
   - Ensure content parity
   - Validate all examples
3. Optional: Test PDF generation: `poetry run make latexpdf`

2.1.5 Questions?

Open an issue in the repository or contact the maintainers.

2.1.6 Français

English version

2.1.7 Comment Contribuer

Nous accueillons les contributions à CIPHER! Voici comment vous pouvez aider:

1. Créez une copie du dépôt
2. Créez une nouvelle branche
3. Ajoutez votre documentation de protocole
4. Soumettez une demande de fusion

2.1.8 Normes de Documentation

Structure du Protocole

- ID de protocole alphanumérique de 5 caractères (générer avec: `python3 -c "import random, string; print(''.join(random.choices(string.ascii_uppercase + string.digits, k=5)))"`)
- Contenu bilingue (anglais et français)
- Références croisées entre versions linguistiques
- Suivre les normes de formatage RST:
  - Guide RST Sphinx
  - Documentation RST

Sections Requises

1. Aperçu:
   - Objectif et description de base
   - Liens vers outils/références pertinents
   - Déclaration de flexibilité du protocole
2. Procédure Opérationnelle Standard:
   - Initialisation
   - Format de Transmission
   - Exemple de Transmission
3. Détails d'Implémentation:
   - Procédure principale

- Exemples avec données de test
- Tables de consultation si nécessaire

4. Considérations de Sécurité:
   - Limites de sécurité
   - Cas d'utilisation prévus

2.1.9 Tests

Avant de soumettre:

1. Construire la documentation localement:

   Installer les dépendances: `poetry install`

   Construire la documentation: `cd docs && poetry run make html`
2. Vérifier les deux versions linguistiques:
   - Vérifier les références croisées
   - Assurer la parité du contenu
   - Valider tous les exemples
3. Optionnel: Tester la génération PDF: `poetry run make latexpdf`

2.1.10 Questions?

Ouvrez un ticket dans le dépôt ou contactez les mainteneurs.

2.2 ROT over Voice Protocol / Protocole ROT sur Voix

Note

Protocol ID/ID de Protocole
Y3IGU

Version
v1.0.1

Updated At/Mis à Jour le
2024-11-28

2.2.1 English

Accéder à la *version française*

Overview

ROT is a simple substitution cipher that replaces each letter with another letter N positions after it in the alphabet. While ROT13 is traditional (N=13), this specification supports any agreed-upon value of N. For testing or implementation, operators may use CyberChef's ROT13 tool.

For amateur radio voice communications, this specification defines a standard operating procedure for its use. Operators may deviate from the specific procedures described here, provided they:

1. Maintain sufficient information for message decryption
2. Stay within the spirit of clear and transparent communication
3. Ensure both parties understand the encoding method being used

Standard Operating Procedure

Initialization

1. Signal intention to begin ROT procedure and specify N value if not 13 Example: "INITIATING ROT13 PROCEDURE" or "INITIATING ROT20 PROCEDURE"

Transmission Format

- Signal the start of an encoded message Example: "CIPHER FOLLOWS"
- Speak each word clearly using ITU phonetic alphabet
- Signal the end of encoded transmission Example: "CIPHER ENDS"

Example Transmission

```
OPERATOR 1: "INITIATING ROT20 PROCEDURE"
OPERATOR 2: "ROT20 ACKNOWLEDGED"
OPERATOR 1: "CIPHER FOLLOWS"
OPERATOR 1: "HOTEL ECHO LIMA LIMA OSCAR"
OPERATOR 1: "CIPHER ENDS"
```

Implementation Details

Encryption and Decryption

To encrypt a message:

1. For each letter in the original message:
    - Count forward N positions in the alphabet
    - Wrap around to 'A' after 'Z'
    - Numbers and special characters remain unchanged
2. Example with N=13:
    - "HELLO" → "URYYB"

- "ABC" with N=2 → "CDE"
- "Z" with N=1 → "A"

To decrypt a message:

1. For each letter in the encoded message:
    - Count backward N positions in the alphabet
    - Wrap around to 'Z' after 'A'
    - Numbers and special characters remain unchanged
2. Example with N=13:
    - "URYYB" → "HELLO"
    - "CDE" with N=2 → "ABC"
    - "A" with N=1 → "Z"

Formula:

$$\textbf{Encryption: } E(x) = (x + N) \bmod 26,$$
$$\textbf{Decryption: } D(x) = (x - N + 26) \bmod 26,$$

where $x \in \mathbb{Z}_{26}$ represents the position of a letter in $X = \{A, B, \ldots, Z\}$,
$x = 0$ corresponds to A,
$N \in \{1, 2, \ldots, 25\}$ is the shift value.

Selecting N Value

- Any value of N from 1 to 25 is valid
- N=13 is traditional and recommended for general use
- Both stations must agree on N value before transmission
- N value may be changed mid-session with mutual agreement

Alphabet Mapping Example (N=13)

Original	Encoded	Original	Encoded
A	N	N	A
B	O	O	B
C	P	P	C
D	Q	Q	D
E	R	R	E
F	S	S	F
G	T	T	G
H	U	U	H
I	V	V	I
J	W	W	J
K	X	X	K
L	Y	Y	L
M	Z	Z	M

Security Considerations

- ROT-N, regardless of N value, is not secure encryption
- Different N values do not significantly increase security
- Use only for training, recreation, or basic privacy
- Consider N value public information, not a secret key

2.2.2 Français

Access the *English version*

Aperçu

ROT est un chiffrement par substitution simple qui remplace chaque lettre par la lettre située N positions après elle dans l'alphabet (Détails ROT13). Bien que ROT13 soit traditionnel (N=13), cette spécification prend en charge toute valeur convenue de N. Pour les tests ou l'implémentation, les opérateurs peuvent utiliser l'outil ROT13 de CyberChef.

Pour les communications vocales en radio amateur, cette spécification définit une procédure opérationnelle standard. Les opérateurs peuvent s'écarter des procédures spécifiques décrites ici, à condition de :

1. Maintenir des informations suffisantes pour le déchiffrement des messages
2. Rester dans l'esprit d'une communication claire et transparente
3. S'assurer que les deux parties comprennent la méthode d'encodage utilisée

Procédure Opérationnelle Standard

Initialisation

1. Signaler l'intention de commencer la procédure ROT et spécifier la valeur N si différente de 13 Exemple : "INITIATION PROCÉDURE ROT13" ou "INITIATION PROCÉDURE ROT20"

Format de Transmission

- Signaler le début d'un message encodé Exemple : "CHIFFREMENT SUIT"
- Épeler chaque mot clairement en utilisant l'alphabet phonétique ITU
- Signaler la fin de la transmission encodée Exemple : "FIN DU CHIFFREMENT"

Exemple de Transmission

```
OPÉRATEUR 1 : "INITIATION PROCÉDURE ROT20"
OPÉRATEUR 2 : "ROT20 CONFIRMÉ"
OPÉRATEUR 1 : "CHIFFREMENT SUIT"
OPÉRATEUR 1 : "HOTEL ECHO LIMA LIMA OSCAR"
OPÉRATEUR 1 : "FIN DU CHIFFREMENT"
```

Détails d'Implémentation

Chiffrement et Déchiffrement

Pour chiffrer un message :

1. Pour chaque lettre du message original :
    - Compter N positions en avant dans l'alphabet
    - Revenir à 'A' après 'Z'
    - Les chiffres et caractères spéciaux restent inchangés
2. Exemple avec N=13 :
    - "HELLO" → "URYYB"
    - "ABC" avec N=2 → "CDE"
    - "Z" avec N=1 → "A"

Pour déchiffrer un message :

1. Pour chaque lettre du message encodé :
    - Compter N positions en arrière dans l'alphabet
    - Revenir à 'Z' après 'A'
    - Les chiffres et caractères spéciaux restent inchangés
2. Exemple avec N=13 :

- "URYYB" → "HELLO"
- "CDE" avec N=2 → "ABC"
- "A" avec N=1 → "Z"

Formule :

$$\textbf{Chiffrement :}\ E(x) = (x + N) \bmod 26,$$
$$\textbf{Déchiffrement :}\ D(x) = (x - N + 26) \bmod 26,$$

où $x \in \mathbb{Z}_{26}$ représente la position d'une lettre dans $X = \{A, B, \ldots, Z\}$,
$x = 0$ correspond à A,
$N \in \{1, 2, \ldots, 25\}$ est la valeur de décalage.

Sélection de la Valeur N

- Toute valeur de N de 1 à 25 est valide
- N=13 est traditionnel et recommandé pour l'usage général

Table de Correspondance Alphabétique Exemple (N=13)

Original	Encodé	Original	Encodé
A	N	N	A
B	O	O	B
C	P	P	C
D	Q	Q	D
E	R	R	E
F	S	S	F
G	T	T	G
H	U	U	H
I	V	V	I
J	W	W	J
K	X	X	K
L	Y	Y	L
M	Z	Z	M

Considérations de Sécurité

- ROT-N, quelle que soit la valeur de N, n'est pas un chiffrement sécurisé
- Différentes valeurs de N n'augmentent pas significativement la sécurité
- Utiliser uniquement pour la formation, le loisir ou la confidentialité de base
- Considérer la valeur N comme une information publique, non comme une clé secrète