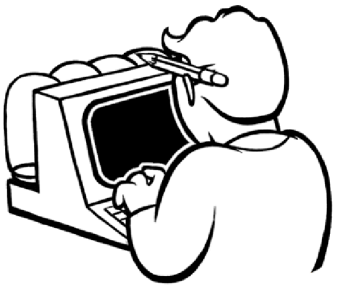
VAULT-TEC

MANUEL DES PROGRAMMEURS

Guide de l'infiltration informatique



STRASBOURG, FR © 2077 VAULT-TEC INDUSTRIES
PUBLIÉ PAR LE DÉPARTEMENT DE LA DOCUMENTATION DE VAULT-TEC

VDSG CE HCK-108-403

Tous les visuels, représentations et projections ont été développés grâce à la science.

Dans l'éventualité d'une catastrophe nucléaire, vous pourriez être amené à devoir reconstruire notre grande nation. C'est pourquoi, Vault-Tec Europe vous a préparé cette documentation éducative afin de vous aider à mieux comprendre les compétences majeures qui font de vous quelqu'un de... SPECIAL.

Aujourd'hui, nous allons parler d'hacking.

Félicitations ! Si vous avez aujourd'hui ce petit livret entre les mains, c'est que vous avez la joie, l'honneur et le privilège d'être un Programmeur.

Votre cerveau se met en ébullition face à un écran et un clavier. Là où beaucoup voient des machines complexes, vous y voyez des merveilles de technologie. Vous pouvez accéder aux archives de l'ancien monde et à ses secrets ! Vous êtes la pierre angulaire de la reconstruction de notre belle nation. Contrairement aux autres parasites qui peuplent nos belles contrées.

MATÉRIEL ET ÉQUIPEMENT

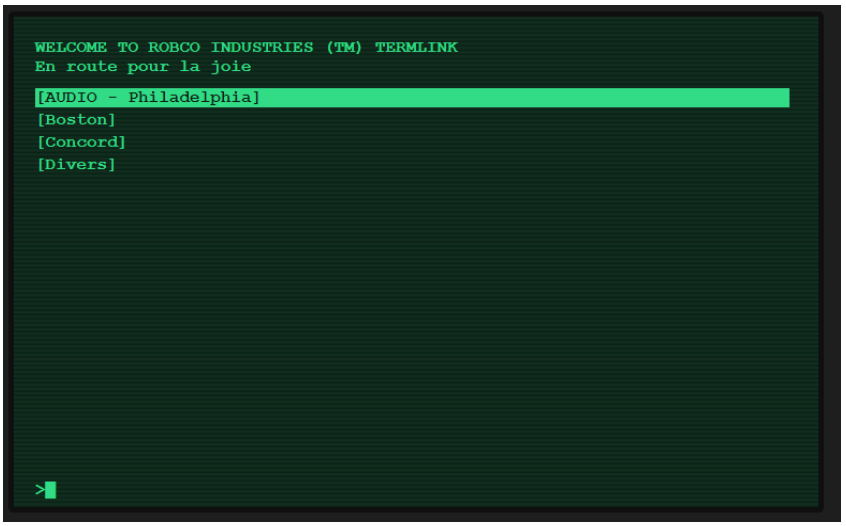
Vous n'avez besoin que de votre cerveau pour re-configurer les équipements d'avant-guerre. S'ils ne sont pas équipés des périphériques nécessaires, vous perdez sans doute votre temps ou bien, vous avez manqué quelque chose.

TERMINAUX ROBCO INDUSTRIES

Les terminaux Vault-Tec fonctionnent majoritairement avec la même interface utilisateur.
Ils permettent de stocker des fichiers textes et audios. La capacité à organiser dans des dossiers et à stocker sur des périphériques de stockages externes, les holobandes, font de cet outil un incontournable !

L'explorateur

Il s'agit de l'écran principal de visualisation des informations.
En plus des caractères d'écriture de votre clavier, vous pourrez naviguer avec les FLÈCHES DIRECTIONNELLES, la touche ENTRÉE et la touche ECHAP.



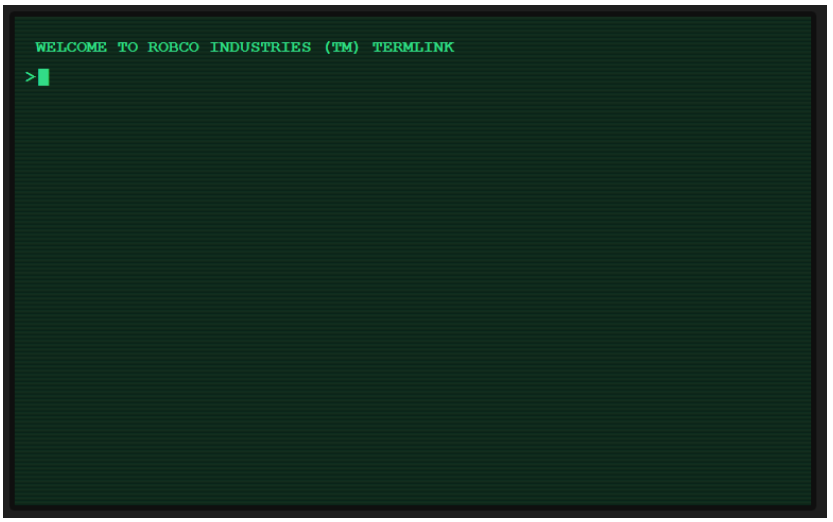
FLÈCHES DIRECTIONNELLES : permet de mettre en surbrillance un dossier, un fichier ou un événement dans l'explorateur.
ENTRÉE : permet de lire le fichier texte ou audio en surbrillance. S'il s'agit d'un dossier, son contenu sera affiché. S'il s'agit d'un événement, celui-ci sera déclenché.
ECHAP : si vous êtes dans un sous-dossier ou en train de lire un fichier, vous revenez en arrière.

SÉCURITÉ ET ACCÈS

Sachez cependant que pour des raisons évidentes de sécurité, les terminaux sensibles sont protégés par des mots de passe bien sûr. Pas de panique, ce guide est là pour ça.

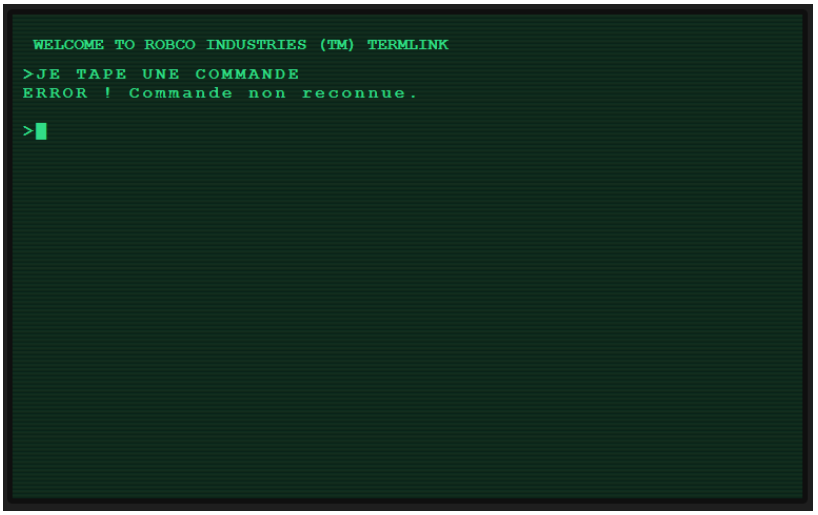
Invite de commande

Si le terminal est protégé, vous arriverez sur l'invite de commande :



Il existe des routines de plusieurs commandes qu'il faut taper à la suite sans se tromper pour réaliser des actions qui mèneront au déverrouillage du poste.

Il faut taper chaque commande une à une dans l'invite en les succédant par un appui sur la touche ENTRÉE pour les valider.



Accéder à un terminal

Rappel des commandes principales, que vous connaissez déjà si vous avez suivi les cours de votre manuel de survie. Vous en apprendrez peut-être d'autres, sait-on jamais.

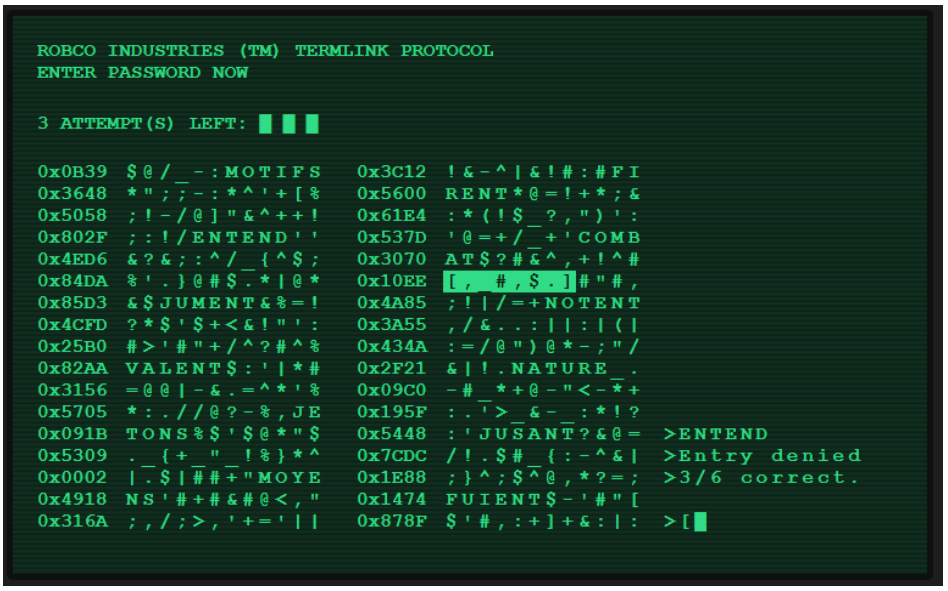
Récupération de numéro de série du terminal :

1. FDISK;F // On demande à obtenir le numéro de série de l'appareil sur lequel on se trouve actuellement

Hackage d'un terminal :

1. SET TERMINAL INQUIRE <NUMERO SERIE> // On signale que des commandes séries vont être tapées
2. SET FILE PROTECTION OWNER:RWED ACCOUNTS;F // On supprime la protection du propriétaire au profit du groupe de maintenance
3. SET HALT MAINT // On force un mode maintenance fictif
4. RUN DEBUG ACCOUNTS;F // On force l'accès en mode debug

À l'issue des commandes réussies, il va falloir trouver le bon mot de passe auto-généré pour la maintenance.
La difficulté dépendra du niveau d'accréditation du terminal. Ce sujet sera abordé plus en profondeur dans la prochaine partie de ce guide.



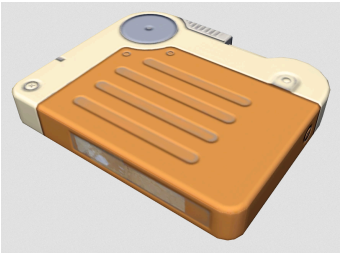
Grâce aux FLÈCHES DIRECTIONNELLES, vous pourrez vous déplacer dans ces lignes de caractères. Avec la touche ENTRÉE, vous pouvez valider un mot mis en surbrillance.
Chaque mot partage un certain nombre de lettres communes entre eux. En bas à droite, à chaque choix de mot, le système vous dira combien de lettres sont bonnes par rapport au bon mot de passe.

Un des mots est le bon mot de passe. Peut-être aurez-vous de la chance du premier coup !

Certains groupes de caractères peuvent se mettre en surbrillance. Essayez de valider, vous aurez une surprise.

Si vous ne trouvez pas la solution, il faudra tout recommencer. Je n'aimerais pas être à votre place.
Cependant, si vous êtes doués, vous accéderez à l'explorateur !
N'oubliez pas de taper la commande **EXIT** dans l'explorateur pour re-sécuriser le terminal. Vous ne voudriez pas que les informations soient en libre accès à tout le monde. Les informations, c'est précieux.

LES HOLOBANDES



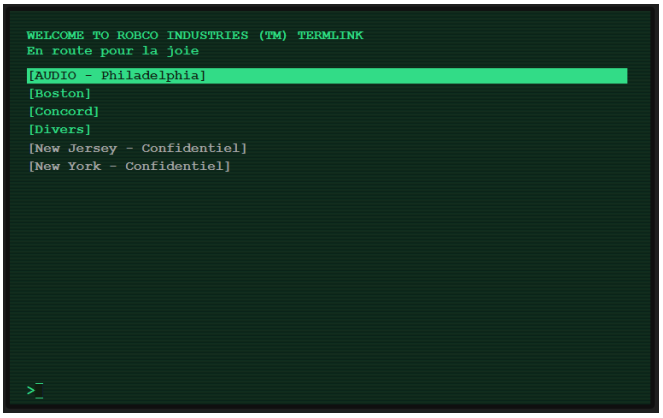
Les holobandes sont des périphériques de stockage externes.

Pour lire leur contenu, il faudra les insérer dans un lecteur prévu à cet effet.

Si vous avez de la chance, votre terminal en sera pourvu.

NOTE HORS-JEU : il est <u>vraiment vraiment</u> interdit de débrancher un lecteur d'un terminal.

Si le niveau d'accréditation du terminal le permet, de nouveaux dossiers et fichiers apparaîtront dans l'explorateur. Dans le cas contraire, ils apparaîtront aussi, mais seront grisés avec une indication d'accréditation.



Voici un rappel des commandes pour modifier l'accréditation du terminal.

Ces commandes sont à effectuer dans l'invite de commande seulement. **Elles ne fonctionnent pas dans l'explorateur.**

Affichage du niveau d'accréditation actuel :

1. SUDO ECHO DIFF;ID <NUMERO SERIE>

Augmentation de l'accréditation (possible qu'une fois toutes les 2 minutes) :

1. SUDO RESIZEUP;ID <NUMERO SERIE>

Diminution de l'accréditation (possible qu'une fois toutes les 2 minutes) :

1. SUDO RESIZEDOWN;ID <NUMERO SERIE>

Notez bien que plus un terminal à un haut niveau d'accréditation, plus le piratage sera difficile.

Rappel important ! La valeur qui remplacera <NUMERO SERIE> dans votre commande s'obtient par la commande disponible au chapitre " Accéder à un terminal : Récupération de numéro de série du terminal ".

LES BADGE D'ACCÈS

Attention, chacune des pièces des abris ne sont pas en libre accès.

Si vous voyez un lecteur de badge à côté d'une porte, c'est qu'il va falloir :

1. Avoir un badge
2. Avoir un badge qui autorise l'accès !

Vous avez plus d'un tour dans votre sac. Vous savez que chaque abri est doté d'au moins un configurateur de badge et de lecteur, relié à un terminal. En général dans l'endroit le plus sécurisé.

Il existe 2 niveaux de protections possibles sur une porte ou un objet sécurisé :

1. Niveau 1 : la protection se trouve au niveau du badge. // il faut pirater le badge
2. Niveau 2 : la protection est au niveau du lecteur (collier de sécurité) ou lecteur + badge (porte sécurisée). // il faut pirater le lecteur

Les lecteurs sont toujours dans des boîtes noires avec deux leds (rouge et verte) et une antenne.

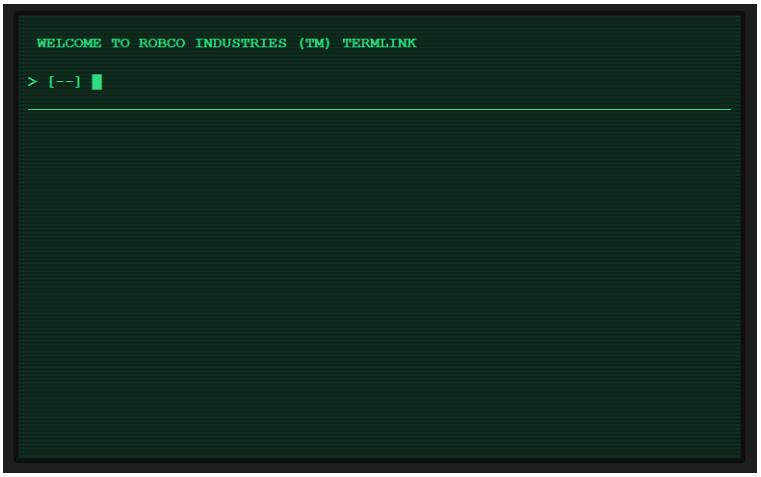
Pirater un badge (Niveau intermédiaire)

Imaginons que vous êtes doués. Vous avez un badge et un terminal avec un configurateur.

Depuis l'invite de commande du terminal, il va falloir ouvrir l'interface du configurateur.

Ouverture de l'interface du configurateur :

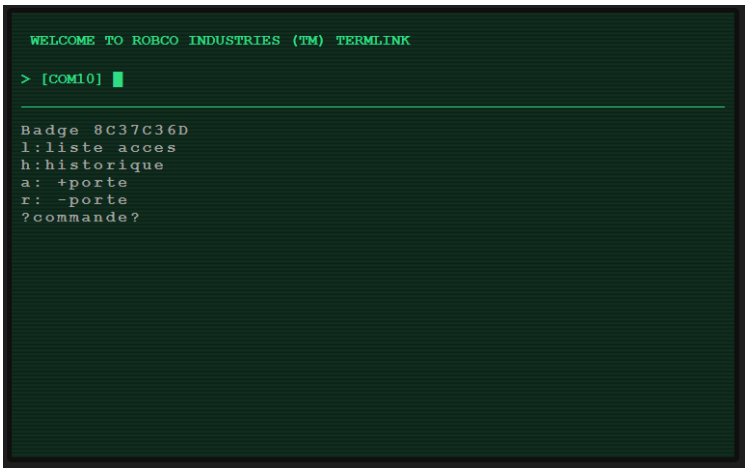
1. OPEN CONFIG ACCESS



Pour pirater le badge, il va falloir poser votre badge sur le configurateur et le laisser pendant toute la manipulation.

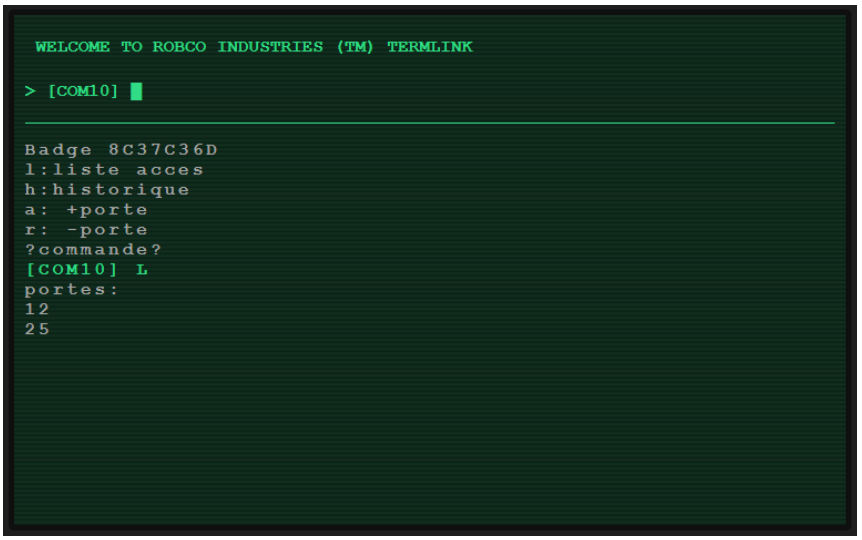
À ce stade, sur le terminal, s'affiche :

- le numéro du badge
- la liste des commandes disponibles :
    - l : liste les numéros de lecteur auquel le badge a accès
    - h : affiche l'historique récent de l'utilisation du badge
    - a : permet d'ajouter un accès à une porte sur le badge (Niveau 1 de protection piraté)
    - r : permet de supprimer l'accès à une porte sur le badge (Niveau 1 de protection piraté)



Pour les commandes de piratage (a et r), il va falloir fournir le numéro du lecteur de badge, mais aussi un mot de passe lié au système de sécurité utilisé.

En **annexe**, le document **système**, liste des mots de passe possibles pour différents systèmes de contrôle d'accès encore utilisés. Pour chaque système, nous connaissons une liste de 15 mots de passe possibles. Il vous faudra trouver le bon.



Utilisation de la commande L pour afficher la liste des portes accessibles avec le badge 8C37C36D

Pirater un lecteur (Niveau avancé)

Attention, le niveau 2 de protection est particulièrement difficile. Il nécessitera de connaître les **MATHÉMATIQUES DU PROGRAMMEUR** en **ANNEXE** pour le **CALCUL DU CODE PIRATAGE** en **ANNEXE** aussi.

Il va vous falloir 4 informations pour mener à bien votre opération :

1. Le code de télécommande : il va falloir repérer le modèle du système de sécurité pour trouver son code de télécommande dans l'**annexe** de ce manuel. (6 caractères)
   Par exemple, pour le système AccesPlus, le code de télécommande est : D56FC3.
2. Le numéro du badge : s'affiche dans l'interface quand vous utilisez le configurateur (8 caractères)
   Exemple : **8C 37 C3 6D**
   NOTE: dans la cas d'un collier de sécurité, prendre 00 00 00 00
3. Le code commande : voici la liste des codes commandes disponibles (1 chiffre)
   a. Ajouter un badge : 1
   b. Retirer un badge de la mémoire d'un lecteur (ni autorisé, ni refusé) : 2
   c. Refuser un badge (même s'il est autorisé dans le badge !) : 3
   d. Ouverture (" accès autorisé ") : 4
   e. Verrouiller : 6
   f. Ouvrir (bloqué en ouverture) : 7
   g. Alarme : 8
   h. Remise à zéro : 9
   NOTE: dans le cas d'un collier de sécurité utiliser "Ouvrir – bloqué en ouverture"
4. Le numéro du lecteur de badge se trouvant sur la porte souhaitée. (1 nombre)

SI vous êtes arrivés ici, c'est que vous avez toutes les informations nécessaires pour le code de piratage du badge ! Vous remarquerez qu'il y a beaucoup de possibilités suivant l'action voulue, le lecteur de badge, le badge et le modèle du configurateur.

Reprenons. Vous êtes dans l'interface. Il va falloir inscrire le code de piratage du badge à partir des 4 informations ci-dessus précédée de la commande **s**. C'est une commande cachée.
Ce qui donne : *s<codePiratage>*

Exemple : **sD56FC3BB6DE2**

La deuxième étape consiste à trouver ce code de piratage à partir des 4 informations ci-dessus.

1. Commençons par traduire tous nos éléments en binaire sauf le code de télécommande:
    a. Code de télécommande. Exemple : D56FC3
    b. Numéro du badge. On convertit et on ne gagne que les 6 derniers chiffres (bits) Exemple: **8C 37 C3 6D -> 10001100001101111100001101101101 -> 1101101101**
    c. Code commande, toujours 4 chiffres (4bits). Exemple: **7 -> 0111**
    d. Numéro du lecteur de badge. On prend toujours 6 chiffres. Exemple:
    34 -> 100010
    7 -> 0111 -> 000111 (on complète avec des 0 devant pour faire 6 chiffres)
    63 -> 111111 -> 111111
2. On cherche les deux bits de parité nécessaires:
    a. Bit parité du badge. On prend le code binaire du badge -> **1101101101**
    On compte le nombre de 1 présent. Ici il y en a 7. Si c'est impaire, alors la réponse est 1 sinon elle est 0.
    Ici la réponse est donc 1
    b. Bit parité du lecteur + commande. On prend les codes binaires du lecteur et de la commande -> 100010 0111
    On compte le nombre de 1 présent. Ici il y en 5. C'est impaire, donc la réponse est 1.
3. Le code binaire finale est donc:
    10 + bitParitéBadge + codeBadge + bitParitéLecteurCommande + commande + lecteur
    10 + 1 + 1101101101 + 1 + 0111 + 100010
4. On regroupe les éléments par groupe de 4 pour reconvertir tout ça en hexadécimal
    1011 1011 0110 1101 1110 0010
    B B 6 D E 2
5. Le code final est donc D56FC3 BB6DE2. Soit la commande a taper: **sD56FC3BB6DE2** dans notre exemple.
6. Si votre code est bon:
    a. Vous piratez un lecteur + badge: félicitation ! Votre badge est piraté, allez l'essayer !
    b. Vous piratez un lecteur de collier de sécurité. Il faut que l'objet soit proche du terminal. **Vous verrez alors la LED rouge s'éteindre et la LED verte s'allumer**. Félicitations !

Vous pouvez consulter le **CALCUL DU CODE PIRATAGE** en **ANNEXE** pour plus de précision et pour trouver les tables de conversion dont vous aurez besoin.

Bonne chance programmeur.

ANNEXES - LES MATHÉMATIQUES DU PROGRAMMEUR

Ce chapitre peut vous servir pour un piratage avancé !

Apprendre à compter

Généralement, on compte en décimal (=base 10). Cela signifie qu'il y a 10 unités possibles (0 à 9). Un ordinateur, ou habituellement une machine électronique, compte en binaire : les 2 seules unités possibles sont 0 et 1.
Et de la même manière qu'en décimal, pour compter au-delà, on ajoute des unités (qu'on appelle alors dizaines, centaines...) ! En décimal, après le 9 (qui peut s'écrire 009, c'est la même chose), on recommence à 0, et on augmente l'unité précédente, ce qui fait 10.

En binaire, c'est pareil : après 001, on passe à 010, puis 011, puis 100. Et voilà !
Avouons-le, ça devient vite très long quand on arrive à des nombres (décimaux) importants.

Par exemple :

- 100 : en binaire, ça fait 1100100.
- 10 000 s'écrit 10011100010000.

Vous suivez ?

Déjà, on va regrouper les unités par 4, et ajouter des 0 à l'avant (comme en décimal, 009=9)10 000 s'écrirait 0010 0111 0001 0000.
Ça fait long !
Pour des raisons de lisibilité et de praticité, on considère que l'ordinateur compte en hexadécimal, c'est-à-dire en base 16.

Par contre, comment compte-t-on après 9, tout en restant sur une unité ? Tout simplement, on va utiliser des lettres : ainsi, après 9 vient A, puis B, C, D, E et F (avec le F, on est alors à 16 unités possibles : 10 chiffres, 6 lettres)

L'avantage, c'est que la conversion binaire <-> hexadécimal se fait très facilement : tout simplement par groupe de 4 chiffres binaires.

En combinant les 2 tables suivantes, on pourra tout faire !

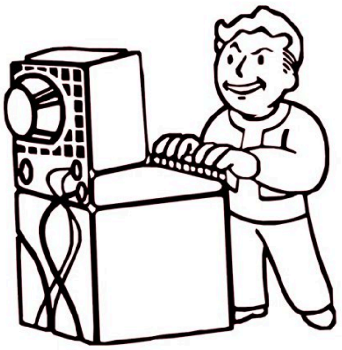


Table de conversion décimal-hexadécimal (base 10 à base 16 et inversement)

dec	hex	dec	hex	dec	hex	dec	hex	dec	hex	dec	hex	dec	hex	dec	hex
0	0	32	20	64	40	96	60	128	80	160	A0	192	C0	224	E0
1	1	33	21	65	41	97	61	129	81	161	A1	193	C1	225	E1
2	2	34	22	66	42	98	62	130	82	162	A2	194	C2	226	E2
3	3	35	23	67	43	99	63	131	83	163	A3	195	C3	227	E3
4	4	36	24	68	44	100	64	132	84	164	A4	196	C4	228	
5	5	37	25	69	45	101	65	133	85	165	A5	197	C5	229	E5
6	6	38	26	70	46	102	66	134	86	166	A6	198	C6	230	E6
7	7	39	27	71	47	103	67	135	87	167	A7	199	C7	231	E7
8	8	40	28	72	48	104	68	136	88	168	A8	200	C8	232	E8
9	9	41	29	73	49	105	69	137	89	169	A9	201	C9	233	E9
10	0A	42	2A	74	4A	106	6A	138	8A	170	AA	202	CA	234	EA
11	0B	43	2B	75	4B	107	6B	139	8B	171	AB	203	CB	235	EB
12	0C	44	2C	76	4C	108	6C	140	8C	172	AC	204	CC	236	EC
13	0D	45	2D	77	4D	109	6D	141	8D	173	AD	205	CD	237	ED
14	0E	46	2E	78	4E	110	6E	142	8E	174	AE	206	CE	238	EE
15	0F	47	2F	79	4F	111	6F	143	8F	175	AF	207	CF	239	EF
16	10	48	30	80	50	112	70	144	90	176	B0	208	D0	240	F0
17	11	49	31	81	51	113	71	145	91	177	B1	209	D1	241	F1
18	12	50	32	82	52	114	72	146	92	178	B2	210	D2	242	F2
19	13	51	33	83	53	115	73	147	93	179	B3	211	D3	243	F3
20	14	52	34	84	54	116	74	148	94	180	B4	212	D4	244	F4
21	15	53	35	85	55	117	75	149	95	181	B5	213	D5	245	F5
22	16	54	36	86	56	118	76	150	96	182	B6	214	D6	246	F6
23	17	55	37	87	57	119	77	151	97	183	B7	215	D7	247	F7
24	18	56	38	88	58	120	78	152	98	184	B8	216	D8	248	F8
25	19	57	39	89	59	121	79	153	99	185	B9	217	D9	249	F9
26	1A	58	3A	90	5A	122	7A	154	9A	186	BA	218	DA	250	FA
27	1B	59	3B	91	55	123	7B	155	9B	187	BB	219	DB	251	FB
28	1C	60	3C	92	5C	124	7C	156	9C	188	BC	220	DC	252	FC
29	1D	61	3D	93	5D	125	7D	157	9D	189	BD	221	DD	253	FD
30	1E	62	3E	94	5E	126	7E	158	9E	190	BE	222	DE	254	FE
31	1F	63	3F	95	5F	127	7F	159	9F	191	BF	223	DF	255	FF
														256	100

Conversion binaire-hexadécimal (base 16 à base 2 et inversement)

En regroupant les bits par 4, depuis la droite, utiliser la table suivante :

binaire	hexa	binaire	hexa	binaire	hexa	binaire	hexa
0000	0	0100	4	1000	8	1100	C
0001	1	0101	5	1001	9	1101	D
0010	2	0110	6	1010	A	1110	E
0011	3	0111	7	1011	B	1111	F

Ainsi, notre 10 000 de tout à l'heure (en binaire 0010 0111 0001 0000) s'écrit en hexadécimal 2710.

Calculer un bit de parité

Un bit de parité permet de détecter simplement des erreurs de saisie ou de transmission. Cela consiste à compter le nombre de bits à 1 dans un mot : si ce nombre est pair, alors le résultat est 0 ; sinon 1. Toutefois, cette technique a des limites : par exemple, une inversion de 2 bits ne sera pas détectée.

Exemples de calcul :
1111 0000
Il y a 4 '1' ; 4 est pair -> parité à 0
10 1010 1010
Il y a 5 '1' ; 5 est impair -> parité à 1
10 1010 1001
Il y a 5 '1' ; 5 est impair -> parité à 1

Opérations Bit à bit

XOR (ou exclusif)

XOR est une opération mathématique binaire, qui consiste à effectuer un " soit l'un, soit l'autre, mais pas les deux ". Autrement dit, les 2 bits doivent être différents pour donner un 1.

1 XOR 0 = 1
0 XOR 1 = 1
1 XOR 1 = 0
0 XOR 0 = 0

Pour comparer des nombres plus longs, on effectue simplement cette opération
bit par bit.
110 XOR 101 = 011
111 XOR 000 = 111
011 XOR 010 = 001

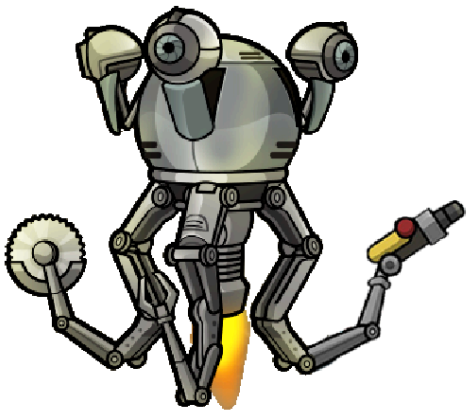
Calculer une somme de contrôle “ checksum XOR ”

Une somme de contrôle permet de détecter simplement des erreurs de saisie/de transmission. Toutefois, contrairement au bit de parité, le résultat est plus long.

La somme de contrôle consiste facilement à effectuer une succession d'opérations XOR sur les différentes valeurs. Elle s'effectue par groupe de 8 bits.
Exemple : $ 4C95 151E soit en binaire : 0100 1100 1001 0101 0001 0101 0001 1110
On effectue une opération XOR sur le bleu et le vert, puis le résultat de cette opération avec le mauve, puis enfin le résultat de cette opération avec le jaune.

0100 1100 XOR 1001 0101 = 1101 1001
1101 1001 XOR 0001 0101 = 1100 1100
1100 1100 XOR 0001 1110 = **1101 0010**

La somme de contrôle est donc **1101 0010**
En fait, on effectue pour chaque “ colonne ” (unité) un calcul de parité ! (opération précédente)
Transformation en hexadécimal : 4C95 151E -> somme de contrôle = D2



ANNEXES - CALCUL DU CODE PIRATAGE

La partie à calculer du code de piratage est un mot codé sur 24 bits. Rappel : un " bit ", c'est 0 ou 1. Rien d'autre.

Pour taper une commande qui concerne un badge, il faut avoir le n° de badge (8 caractères hexadécimaux), dont on ne prendra que les 10 derniers bits (donc : convertir le tout en binaire, ne prendre que les 10 bits les plus à droite) (sinon mettre des 0 à la place).

Pour hacker un lecteur, il faudra son id (numéro) (à trouver, entre 0 et 63) à convertir également en binaire.

10ab bbbb bbbb bcdd ddee eeee

Soit de gauche à droite :

bit[1,2]	'10' obligatoire
bits[3]	bit de parité badge
bits[4..13]	badge
bits[18]	parité lecteur + commande
bits[14..17]	commande (sur 4 bits)
bits [19..24]	id lecteur (6bit)

<u>Le plus simple est de procéder de droite à gauche :</u>

- Avoir l'id (en hexadécimal) du lecteur, à coder sur 6 bits.
- La commande (4 bits) // La plupart des constructeurs utilisent les mêmes commandes principales : (à convertir en binaire sur 4 bits (donc commencer par des 0)
    - Ajouter un badge : 1
    - Retirer un badge de la mémoire d'un lecteur (ni autorisé, ni refusé) : 2
    - Refuser un badge (même s'il est autorisé dans le badge !) : 3
    - Ouverture (" accès autorisé ") : 4
    - Verrouiller : 6
    - Ouvrir (bloqué en ouverture) : 7
    - Alarme : 8
    - Remise à zéro : 9
- Calculer le bit de parité de lecteur-commande (1 bit)
    - **ERR1 si incorrect**
- Ajouter le n° du badge (converti en binaire, les 10 bits de droite uniquement) (ou 00 0000 0000 si pas pour un badge)
- Calculer le bit de parité sur badge

ERR2 si incorrect

- 10

Enfin, convertir le résultat en hexadécimal : le résultat doit faire 6 caractères et commencer par 8,9,A ou B. Sinon c'est que vous vous êtes trompé.

Le code de piratage est la concaténation du code télécommande avec la commande que vous venez de calculer.

Exemple

Je veux que le lecteur n° 19 refuse le badge n° A8 55 33 28

quoi ?	**valeur**	**binaire**
n° du lecteur en hexadécimal	19 (décimal) 13 (hexa)	1⟶0001 ; 3⟶0011 01 0011
Commande	3	0011
Bit de parité lecteur + commande	5 *1 ci-dessus ⟶ 1	1
n° badge... 10 bits seulement	A8 55 33 28	1010 1000 0101 0101 0011 0011 0010 1000
parité badge + r	4 *1 ci-dessus ⟶0	0
10		10

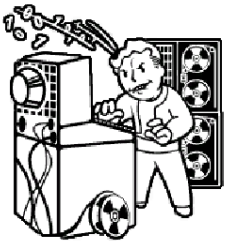
Ce qui fait 1001 1001 0100 0100 1101 0011
Soit en hexa : **9 9 4 4 D 3**

Ensuite, supposons que je sois sur un système AccesPlus, dont le code télécommande est D56FC3 : je tape dans le terminal la commande suivante :

s*D56FC39944D3*

Et voilà !

NOTE HORS-JEU



Conscients de la complexité d'une partie de ce document, nous vous invitons à contacter sur place un organisateur en cas de difficultés extrêmes. Les personnes responsables de votre baisse de tension suite à la lecture de ce document se feront un plaisir de vous guider dans la mise en pratique des instructions citées plus tôt.

Nous ne prenons pas en charge la dispense de soins liés aux migraines et autres douleurs cérébrales. Merci de prévoir vos aspirines en conséquence.

ANNEXES - SYSTÈME

Liste de mots de passe possibles en fonction de la marque/modèle du système.

Système AccesPlus - Code de télécommande : D56FC3 / clé : 144

K35JN2P7	3XZW38T2	GE974D9B
555RC4TR	E9Z56P9Y	5EE73FA6
T4G5Q28E	8P32KXZ4	2C4QHH29
5B77D5GT	H2X7AB95	G8628VSS
4M4RJB73	3PHZ9Q83	66GR5AU3

Système DMB11 - Code de télécommande : 25A601 / clé : 16

JyBdo0B67	CSgD84ed3	dhGZ83Pf7
hk9Yp5W9W	6Yxp7aYW9	loOP4luX6
F4Frir1W4	G2GqOgkJ9	R27GmtQ5r
2i0rel73V	bQ9Fwt37U	7F82LjxTq
63ztXdVZ6	rQOU8yHl9	5P2Yrb8uF

Système MCC2 - Code de télécommande : F9D130 / clé : 48

G9M9z8uw	7NrB86xk	65qNe6Ux
w6a59SgG	Te3M2md3	Z8ii7Ug3
3Kg9r6Kq	48qcjX3N	6R88Tcds
4q4yh6HA	7y55MBem	382DeiqC
Fz2x8Ec9	5Lu9Crg2	iq8uV4Q2

Système SES High - Code de télécommande : B9D6F0 / clé : 78

EXPTRZNSLB	YCKCARNJSL	PONTRHGJLG
XWFREERLXS	RZHWTYQLQU	DMSCHSDWOO
TEHREKHORO	FAWSBXRUBV	LBEVCULWWI
JCPNQHKWMA	DXISQXWNXL	IUWZLRILVT
RZCORVPQLI	YLLMLVTECO	IADWWQRMJM

Consultez régulièrement la documentation fournie par Vault-Tec Europe pour préparer votre survie et répondre à la question :

Qu'est-ce qui fait de vous quelqu'un de... SPECIAL ?

« La science informatique n'est pas plus la science des ordinateurs que l'astronomie n'est celle des télescopes. »