	Serveur 1	Serveur 2	Serveur 3	Serveur 4	Serveur 5			
Configuration	IP : 192.168.2.2 Certificat SSL valide Port 443 ouvert	IP : 192.168.2.3 Certificat SSL révoqué Port 443 ouvert	IP : 192.168.2.4 Certificat SSL non-valide Port 443 ouvert	IP : 192.168.2.5 Certificat SSL valide Doublon avec Serveur 1 Port 443 ouvert	IP : 192.168.2.6 Certificat SSL valide Port 443 fermé Port 444 ouvert	Résultats attendus	Résultats produits	Conclusion
ZMAP – Test sur réseau	X	X	X	X		Fichier produit doit être : 192.168.2.2 192.168.2.3 (?) 192.168.2.4 (?) 192.168.2.5	192.168.2.2 192.168.2.3 192.168.2.5	ZMAP ne liste pas les ports SSL dont le certificat est invalide (service Apache ne démarre pas), par contre il récupère les ports SSL si le certificat est révoqué.
RC (SSL) – Entrées ZMAP = Termine						RC termine (sans constat sur la validité du résultat) avec la liste produite par ZMAP	OK	
RC (SSL) – Test Réseau	X	X	X	X		Un dossier certs contenant le certificat de Serveur1 et Serveur4 (obligatoire), Serveur2 (optionnel). Serveur3 ne doit pas y être. Un dossier keys contenant les clés publiques associées aux certificats stockés.	certs/ . 192.168.2.2.pem . 192.168.2.3.pem . 192.168.2.5.pem keys/ . 192.168.2.2.pem . 192.168.2.3.pem . 192.168.2.5.pem	Tout les certificats sont récupérés
RC (SSL) – Gestion des doublons	X			X		Il doit également gérer les doublons, en créant un répertoire contenant les fingerprint des certificats (pour la gestion des doublons), et un autre contenant les doublons.	certs_doublons/ . <fingerprint Sv1 et Sv4> certs_links/ . <fingerprint Sv1 et Sv4> . <fingerprint Sv2> moduli	La détection des doublons fonctionne

Entier premier choisi parmis une base {p: 2, q: 3, r: 5, s: 7, t: 11, u: 13, v: 17, w: 19}

Factorisation	Entrées	Résultats attendus	Résultats produits
F – Calcul des fils du 1e arbre – nombre impaire (3 modulos) – Sans entier premier identiques [code : F1]	N1=p*q, N2=r*s, N3=t*u, N4 = 1 (par convention)	Fichiers intermédiaires entre chaque niveau, représentant le produit des fils deux par deux (ici un seul : N1*N2 et N3). Fichier final --> N1*N2*N3*1	OK
F – Calcul des fils du 1e arbre – nombre impaire (3 modulos) – Avec entier premier identiques [code : F2]	N1=p*q, N2=q*s, N3=p*u, N4 = 1 (par convention)	Fichiers intermédiaires entre chaque niveau, représentant le produit des fils deux par deux (ici un seul : N1*N2 et N3). Fichier final --> N1*N2*N3*1	OK
F – Calcul des fils du 1e arbre – nombre paire (4 modulos) – Sans entier premier identiques [code : F3]	N1=p*q, N2=r*s, N3=t*u, N4 = v*w	Fichiers intermédiaires entre chaque niveau, représentant le produit des fils deux par deux (ici un seul : N1*N2 et N3*N4). Fichier final --> N1*N2*N3*N4	OK
F – Calcul des fils du 1e arbre – nombre paire (4 modulos) – Avec entier premier identiques [code : F4]	N1=p*q, N2=q*s, N3=v*u, N4 = q*w	Fichiers intermédiaires entre chaque niveau, représentant le produit des fils deux par deux (ici un seul : N1*N2 et N3*N4). Fichier final --> N1*N2*N3*N4	OK
F – Calcul des fils du 2e arbre	Sortie finale de F1	Fichiers intermédiaires entre chaque niveau, représentant le modulo des pères selon les niveaux calculés précédemment (ici deux niveaux : Le premier --> N1*N2*N3 mod (N1*N2)^2 == X1 et N1*N2*N3 mod (N3*1)^2 == X2 Le deuxième --> X1 mod N1^2 == Y1, X1 mod N2^2 == Y2, X2 mod N3^2 == Y3 et X2 mod 1 == Y4.) Fichier final --> GCD(Y1/N1, N1), GCD(Y2/N2, N2), GCD(Y3/N3, N3), GCD(Y4, 1)	OK
F – Calcul des fils du 2e arbre	Sortie finale de F2	Fichiers intermédiaires entre chaque niveau, représentant le modulo des pères selon les niveaux calculés précédemment (ici deux niveaux : Le premier --> N1*N2*N3 mod (N1*N2)^2 == X1 et N1*N2*N3 mod (N3*1)^2 == X2 Le deuxième --> X1 mod N1^2 == Y1, X1 mod N2^2 == Y2, X2 mod N3^2 == Y3 et X2 mod 1 == Y4.) Fichier final --> GCD(Y1/N1, N1), GCD(Y2/N2, N2), GCD(Y3/N3, N3), GCD(Y4, 1)	OK

F – Calcul des fils du 2e arbre	Sortie finale de F3				Fichiers intermédiaires entre chaque niveau, représentant le modulo des pères selon les niveaux calculés précédemment (ici deux niveaux : Le premier --> N1*N2*N3 mod (N1*N2)^2 == X1 et N1*N2*N3 mod (N3*N4)^2 == X2 Le deuxième --> X1 mod N1^2 == Y1, X1 mod N2^2 == Y2, X2 mod N3^2 == Y3 et X2 mod N4^2 == Y4.) Fichier final --> GCD(Y1/N1, N1), GCD(Y2/N2, N2), GCD(Y3/N3, N3), GCD(Y4/N4, N4)	OK			
F – Calcul des fils du 2e arbre	Sortie finale de F4				Fichiers intermédiaires entre chaque niveau, représentant le modulo des pères selon les niveaux calculés précédemment (ici deux niveaux : Le premier --> N1*N2*N3 mod (N1*N2)^2 == X1 et N1*N2*N3 mod (N3*N4)^2 == X2 Le deuxième --> X1 mod N1^2 == Y1, X1 mod N2^2 == Y2, X2 mod N3^2 == Y3 et X2 mod N4^2 == Y4.) Fichier final --> GCD(Y1/N1, N1), GCD(Y2/N2, N2), GCD(Y3/N3, N3), GCD(Y4/N4, N4)	OK			