Préparation RSA

Chaque correspondant doit effectuer les opérations suivantes.

Théorie	**Exemple numérique**
choisir deux nombres premiers (p) et (q) suffisamment grands	$p = 5$ $q = 11$
calculer $n = p \cdot q$ $\boxed{n}$ est appelé le **module** (environ 300 chiffres)	$n = 55$
calculer $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$ $= m$	$m = 4 \cdot 10 = 40$ $(\varphi(n) =)$
choisir un entier naturel e relativement premier à m $\boxed{e}$ est appelé l'**exposant de chiffrement**	$e = 43$
calculer (d) > 0 tel que $d \cdot e \equiv 1 \bmod \varphi(n)$ $\iff d \cdot e + y \cdot m = 1$ (d est l'inverse modulo m de e) d est appelé l'**exposant de déchiffrement**	$d = 43^{-1} \bmod 40$ $\varphi(n)$ $d = 3^{-1} \bmod 40$ $\Leftrightarrow 3d + 40K = 1$ (equation diophantienne) ou $3 \cdot 27 = 1 \bmod 40$ (trouver par tatonnement) $d = 27$

Remarque : Pour ceux que ça intéresse : φ s'appelle la fonction indicatrice d'Euler

Chiffrer

Théorie	Exemple numérique
l'expéditeur connaît $\boxed{n}$ et $\boxed{e}$ du destinataire (clé publique)	$n = 55$ et $e = 43$
transformer le message à envoyer en un entier m tel que $1 < M < n$	"scarabee" $M = 19\ 03\ 01\ 18\ 01\ 02\ 05\ 05$
éventuellement, couper le message en blocs de longueur adéquate	$m_1 = 19$, $m_2 = 03$, $m_3 = 01$, $m_4 = 18$, $m_5 = 01$, $m_6 = 02$, $m_7 = 05$, $m_8 = 05$
chiffrer chaque bloc : le cryptogramme c à transmettre est donné par $C \equiv M^e \bmod n$ c : crypté m : message e : encription	$C = 19^{43} \bmod 55 = 19^{32+8+2+1} \bmod 55$ $= 19^{32} \cdot 19^8 \cdot 19^2 \cdot 19^1 \bmod 55$ $= 39 \bmod 55$ "square and multiply" $19^1 \equiv 19 \bmod 55$ $19^2 \equiv 31 \bmod 55$ $19^4 \equiv 26 \bmod 55$ $19^8 \equiv 16$ " " $19^{16} \equiv 36$ " " $19^{32} \equiv 31$ " " $C = 39\ 27\ 04\ 02\ 01\ 08\ 15\ 15$

Déchiffrer

Théorie	Exemple numérique
le destinataire connaît (p), (q) et (d) (clé privée)	$p = 5$, $q = 11$ et $d = 27$
le destinataire reçoit le cryptogramme C	
pour retrouver le texte clair M, calculer : $M \equiv C^d \bmod n$ d : décription	$39^{27} \bmod 55$ $39^1 \equiv 39 \bmod 55$ $39^2 = 36$ " " $39^4 \equiv 31$ " " $39^8 \equiv 26$ " " $39^{16} \equiv 16$ " " $39^{27} \bmod 55 = 39^{16} \cdot 39^8 \cdot 39^2 \cdot 39^1 \bmod 55$ $= 19 \bmod 55$

RSA avec signature : message à envoyer : "OK" $\iff \mathcal{M} = 15|11 \iff m_1 = 15\,;\, m_2 = 11.$

message en clair $\mathcal{M} \implies$ cryptogramme $\mathcal{C}$ correspondant
$\mathcal{M} \implies$ signature $s \implies$ cryptogramme s_c correspondant
Le destinataire reçoit donc le couple $(c\,;\, s_c)$

	Clé publique	Clé privée
Alice Expéditeur	$n = 65\,;\, e = 11$	$p = 5\,;\, q = 13\,;\, d = 35$
Bob Destinataire	$n = 55\,;\, e = 43$	$p = 5\,;\, q = 11\,;\, d = 27$

Opérations effectuées par l'expéditeur :

chiffrer le message $\mathcal{M} = 15\|11$	signer (et chiffrer) le message $\mathcal{M} = 15\|11$
	1) l'expéditeur signe (chiffre avec sa clé privée) : $s_1 \equiv 15^{35} \mod 65 \equiv 20$ $s_2 \equiv 11^{35} \mod 65 \equiv 6$ $\Rightarrow s = 20\|06$ 2) l'expéditeur chiffre la signature :
$c_1 \equiv 15^{43} \mod 55 \equiv 20$ $c_2 \equiv 11^{43} \mod 55 \equiv 11$ $\Rightarrow \mathcal{C} = 20\|11$	$20^{43} \mod 55 \equiv 25$ $6^{43} \mod 55 \equiv 51$ $\Rightarrow s_c = 25\|51$

Opérations effectuées par le destinataire :

déchiffrer le cryptogramme reçu $\mathcal{C} = 20\|11$	vérifier la signature chiffrée $s_c = 25\|51$
	1) le destinataire déchiffre la signature :
$m_1 \equiv 20^{27} \mod 55 \equiv 15$ $m_2 \equiv 11^{27} \mod 55 \equiv 11$	$25^{27} \mod 55 \equiv 20$ $51^{27} \mod 55 \equiv 6$
	2) le destinataire vérifie la signature :
	$m_1 \equiv 20^{11} \mod 65 \equiv 15$ $m_2 \equiv 6^{11} \mod 65 \equiv 11$
$\Rightarrow \mathcal{M} = 15\|11$	$\Rightarrow \mathcal{M} = 15\|11$