Date	Sujet	Savoirs clés / Exercices- Calculs vus en cours
5 Oct	**Théorie de l'information classique**	Différence entre information quantique et classique, Interféromètre à 1 photon Maitriser les définitions de l'entropie, et de l'information mutuelle, en connaître les propriétés, savoir mettre en œuvre ces connaissances pour résoudre des exercices (exemples vus en cours : anniversaire, test de dépistages) Connaître le principe des théorème de codage de source et de codage de canal, être familier avec la notion de séquence typique et faire le lien avec le codage de source (compression possible jusqu'à l'entropie de la source)
19 Oct	**Théorie de l'information quantique**	Savoir appliquer le formalisme de la matrice densité, de la mesure projective, et de la mesure généralisée (POVM). Faire le lien entre les deux formalisme (purification, Naimark dilation theorm). Savoir calculer une trace partielle (cf exercice) Exercice sur matrice densité, qubit et sphère de Bloch
2 Nov	**Cryptographie Classique et quantique**	Connaître les définitions des principaux services de sécurité : confidentialité, intégrité, authentification, non répudiation, et faire le lien avec des primitives cryptographique Connaître les définitions suivantes et faire le lien avec des algorithmes : sécurité inconditionnelle, calculatoire, cryptographie symétrique, asymétrique. Comprendre le principe du One-Time-Pad et résoudre des exercices (cf cours) sur ses propriétés. Comprendre le dimensionnement d'un algorithme cryptographique et maitriser les ordres de grandeurs (cf cours). Comprendre le fonctionnement de l'algorithme RSA, et les notions de théorie des nombres associées (Th de Fermat, Algo Euclide, Indicatrice d'Euler), et exercices associés (cf fin du cours)
23 Nov	**Distribution quantique de clé (QKD)**	Connaître le théorème de non-clonage et lien avec sécurité de la QKD , les étapes d'un protocole QKD, le détail du protocole BB84 et ceux du protocole de monnaie quantique (Wiesner 1969) Savoir faire le lien opérationnel entre la théorie de l'information (entropie, information mutuelle) et le taux de clé en QKD TD : Attaques indviduelles sur BB84
4 Janvier	**Communications quantiques et applications**	Faire le lien entre hardware de communication quantique et mise en œuvre de la QKD. Savoir faire la différence et comparer CV et DV-QKD. Connaître les ordre de grandeurs importants (pertes, bruit des détecteurs) et le lien avec distance accessible (sur fibre et comparaison avec le spatial). Principes des réseaux quantique, notion de trusted node. Exercice vu en cours : Répéteurs quantiques basés sur entanglement swapping + distillation d'intrication
18 Janv	**Suprématie Quantique**	, ➔ **Pas au programme de l'examen**