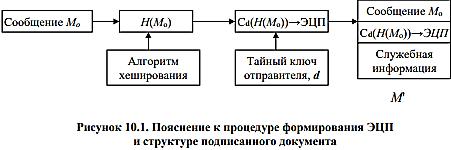
**ЭЦП** – контрольная хар-ка сообщения, кот. вырабат. с исп. личного ключа, провер. с пом. откр. ключа, служит для контроля цел-сти и подлинности сообщения и обесп. невомзожность отказа от авторства **ЭЦП** – бинарная посл-сть символов, явл. реквизитом эл. дока, зависит от его содержания и предн. для подтверждения цел-сти и подлинности эл. дока

**Функции ЭЦП:**  
\* аутент. лицо, подписавшее собщ  
\* контрол. целостности  
\* защищать от подделок  
\* доказать авторство (если отриц)

**Виды ЭЦП:**  
\* *на основе симм. ключей* (с тайным ключом) – как DES  
\* *на основе симм. систем и посредника* – две симм. с-мы: отпр-посред + посред-получ (посредник выдает обоим разный тайный ключ)  
\* *на основе асимм. систем* (с откр. ключом) – эцп как отд. элмента отсутствует, исп. ключевая инфа отправителя: откр. ключ – для зашифр, тайный – для расшифр

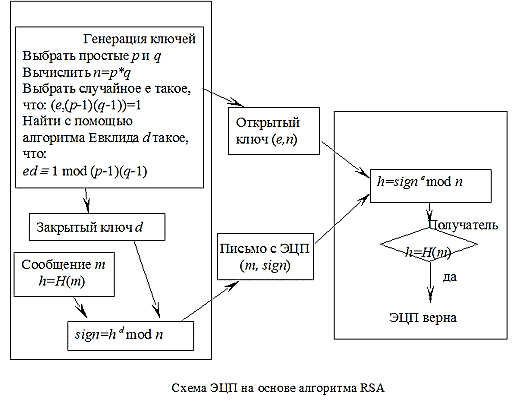
**ЭЦП на основе хэшей подписываемых сообщений:**

  
\* подпис. не само сообщения, а его хэш H(Mo)  
\* подпис. док M’ – конкатенация докаMo + ЭЦП, S  
\* также там мб дата, t отправки …  
\* ЭЦП может проверить каждый, у кого есть *откр. ключ* автора

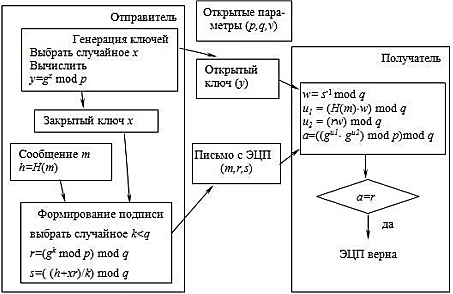
**Генерация ЭЦП:   
отправитель:**\* вычисляет хэш сообщ М - H(M)  
\* вычисляет содержание ЭЦП, S по хешу H(M) с исп. закр.ключа d: S = Cd(H(M))  
\* конкат ЭЦП + М + нек. служебная инфа == M’  
\* посыл. M’ получателю  
**получатель:**  
\* отдел S от М  
\* примен к М хеширование (та же ф-я)  
\* исп. откр. ключ отправителя, расшифр S (извлек из ЭЦП хеш-образ отправленного сообщ)  
\* провер. соответствие (=) обоих хэшов

**ЭЦП на основе RSA:**

**две ситуации:**  
\* сообщ Мо подпис. и передается в откр. виде: S = (H(Mo))d0 mod no  
\* сообщ Мо подпис. и передается в зашифр.: анал., но do,no – эл-ты тайного ключа отпр-ля,  
 перед. сообщ M’=Mo||S  
 *расшифр*: H(Mo) = (S)eo mod no, потом сравн с H(Mп)



**ЭЦП на основе DSA:**

DSA (Digital Signature Algorithm) – алг. цифр. подписи  
\* p – прост. число [64-1024], кратно 64  
\* q [160] – простой множитель (p-1)  
\* g = v(p-1)/g mod p > 1, v – любое число (1, p-1]  
\* y = gX mod p, x<q – закр. ключ  


**ЭЦП Эль Гамаля:**

**Генерация ключ. инфы (p,g,x\*,y):**\* выбир простое p  
\* выбир g<p – первообразный корень числа p  
\* выбир х<p  
\* вычисл. y, y = gXmod p

**Зашифр:** результат – т. одна пара чисел! (не пара для к. блока)  
 это сообщение – хеш подпис. дока  
 \* выбрать k , вз-простое с (p-1)  
 S = {a, b}  
 \* a = gk mod p  
 \* b = k-1 (H(M0) – xa) mod (p-1)  
 получателю отправляют M’ = Mo||S  
**Верификация:** H(Mп) = h – вычисл. хеш полученного сообщ.  
 провер ya \* ab = gh (mod p)

**ЭЦП Шнорра: (РБ)**

как Эль-Гамаль, но число p м. взять поменьше

**Генерация ключевой инфы: (p, g, q, x\*, y)**\* p – простое число [512-1024 бит]  
\* q – простое число [160]  
\* p-1 – делитель  
\* g≠1 – любое число – gq = 1 mod p  
\* x – число <q (закр. ключ) [160+]  
\* y = g–X mod p  
**Подпись сообщения:**  
\* k – случ. число [1, q]  
\* a = gk mod p  
\* h = H(Mo || a) – созд. хеш-образ сообщ-я  
\* b = (k + xh) mod q  
\* отпр. M ’ = Mo||S, S={h,b}  
**Проверка подписи:**  
\* X = gb yh (mod p)  
\* провер рав-во h = H(Mп||X)

**Вопросы для контроля:**

1. Дать определение ЭЦП.   
**ЭЦП** – контрольная хар-ка сообщения, кот. вырабат. с исп. личного ключа, провер. с пом. откр. ключа, служит для контроля цел-сти и подлинности сообщения и обесп. невомзожность отказа от авторства **ЭЦП** – бинарная посл-сть символов, явл. реквизитом эл. дока, зависит от его содержания и предн. для подтверждения цел-сти и подлинности эл. дока

2. Охарактеризовать основные функции ЭЦП.   
\* аутент. лицо, подписавшее собщ  
\* контрол. целостности  
\* защищать от подделок  
\* доказать авторство (если отриц)

3. В чем заключаются сходства и различия между собственноручной и электронной подписью.   
ЭЦП – бин. послед  
рукой – графический образ

4. Охарактеризовать основные способы реализации ЭЦП.   
\* *на основе симм. ключей* (с тайным ключом) – как DES (один ключ для заш и расш)  
\* *на основе симм. систем и посредника* – две симм. с-мы: отпр-посред + посред-получ (посредник выдает обоим разный тайный ключ)  
\* *на основе асимм. систем* (с откр. ключом - RSA) – эцп как отд. элмента отсутствует, исп. ключевая инфа отправителя: откр. ключ – для зашифр, тайный – для расшифр

5. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?

6. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы ЭльГамаля, схемы Шнорра, а также на основе DSA.

rsa – много времеин тратится на модульную арифметику

7. Какие элементы составляют ключевую информацию алгоритмов реализации ЭЦП, перечисленных в п.6?

8. Дать сравнительные характеристики схемам ЭЦП, перечисленным в п.6.

9. Охарактеризовать особенности государственного стандарта ЭЦП в Республике Беларусь